Dikran Dikranjan *Maria Silvia Lucido*

Aritmetica e algebra

Indice

Prefazione

Questo libro è basato sulla nostra esperienza nell'insegnamento dei corsi di Aritmetica e Algebra 1 e 2 al corso di laurea in matematica del nuovo ordinamento presso la Facoltà di Scienze dell'Università di Udine a partire dal 2000. Gli appunti iniziati allora sono la base del libro. La scelta del materiale e la sua quantità è stata determinata e aggiornata nel corso di tali insegnamenti.

La necessità di scrivere un nostro testo anziché usare quelli già esistenti era nata dalle nuove esigenze delle lauree triennali italiane.

Nei primi tre capitoli si introducono i concetti alla base di ogni altro corso di matematica e possono coprire un corso bimestrale di Aritmetica. L'obiettivo del resto del libro è di introdurre le strutture algebriche fondamentali: i semigruppi, i gruppi e gli anelli. I capitoli 4–8 sono pensati per un corso bimestrale di Algebra 1 (gruppi e cenni sulle strutture algebriche), mentre i capitoli 9–12 sono pensati per un corso bimestrale di Algebra 2 (anelli e campi).

Alla fine di ogni capitolo, riportiamo molti esercizi che riguardano il materiale esposto nel capitolo. La lettura del libro deve essere accompagnata da un lavoro serio sugli esercizi. Alcuni di essi, denotati con * sono più difficili e possono essere tralasciati durante una prima lettura del testo. Allo scopo di incoraggiare lo studente a provare a risolvere gli esercizi per conto proprio prima di andare a guardare la soluzione, abbiamo raccolto svolgimenti e suggerimenti nell'ultimo capitolo. Crediamo che possa essere molto utile avere in un unico volume sia il testo che gli esercizi con gli svolgimenti. Il libro ne contiene oltre 500, di cui oltre 300 con soluzione o suggerimento.

Il processo di creare e trasmettere matematica ha due componenti molto diverse: l'idea ispiratrice di ogni dimostrazione è il "cuore" (il nocciolo) che il lettore deve capire e ricordare, mentre la costruzione di un argomento rigoroso è la "spina dorsale" senza la quale non è possibile trasmettere correttamente la dimostrazione. Abbiamo cercato, per quanto possibile, di dare l'idea principale della dimostrazione in un breve commento iniziale e poi esporre con rigore tutti i dettagli della dimostrazione stessa. Laddove questo non è stato fatto, consigliamo al lettore di farlo. Tutte le dimostrazioni terminano con □, per permettere una lettura più agevole del testo.

rappresentazione come prodotto diretto di gruppi ciclici. Si calcolano inoltre i gruppi di automorfismi dei gruppi ciclici.

Nel capitolo 8 si affrontano le proprietà dei gruppi non abeliani. Si considerano vari modi di "misurare" la mancanza di commutatività del gruppo (il sottogruppo derivato, i centralizzanti, i normalizzanti, ecc.). Si provano l'equazione delle classi, il lemma di Cauchy ed il primo teorema di Sylow per i gruppi finiti. Dimostriamo inoltre che il gruppo alterno A_n è semplice per $n > 4$. Concludiamo questo capitolo con le azioni di gruppi che permettono di dare una dimostrazione diversa del primo teorema di Sylow e di dimostrare il secondo e il terzo teorema di Sylow.

L'obiettivo dei capitoli 9–12 è di studiare le strutture algebriche con due operazioni: gli anelli e i campi. È richiesta la conoscenza della teoria dei gruppi abeliani esposta nei capitoli 6–7 e la conoscenza delle proprietà principali degli spazi vettoriali studiate nei corsi di geometria e richiamate nel paragrafo 4.5.

Nel capitolo 9 analizziamo gli anelli e le sottostrutture ad essi associate: sottoanelli, ideali e quozienti. Vengono inoltre definiti gli ideali primi e gli ideali massimali di un anello commutativo e ne viene data una caratterizzazione attraverso l'anello quoziente. Dimostriamo il teorema di Krull, che garantisce l'esistenza di ideali massimali negli anelli commutativi unitari. Introduciamo i quaternioni, i numeri particolari "quattro-dimensionali" inventati dal matematico irlandese William Rowan Hamilton (1805-1865) 160 anni fa con molte applicazioni in geometria, in meccanica razionale e in fisica.

Il capitolo 10 è dedicato ai prodotti diretti e al concetto di omomorfismo di anello. Motivati dal passaggio dal dominio $\mathbb{Z}$ al suo campo dei quozienti $\mathbb{Q}$, si dimostra che ogni dominio ammette un campo dei quozienti. In questo capitolo introduciamo anche i reticoli e le algebre di Boole come strutture algebriche. Dimostriamo che ogni reticolo distributivo e limitato si può rappresentare come un reticolo di sottoinsiemi di un dato insieme. Questo paragrafo può essere tralasciato durante una prima lettura del testo.

Nel capitolo 11 viene introdotta una costruzione specifica per gli anelli: l'anello di polinomi e si descrivono in modo più approfondito i domini, anelli commutativi unitari senza divisori dello zero. Si studiano i domini che soddisfano il teorema fondamentale dell'aritmetica, cioè i domini in cui ogni elemento non invertibile si fattorizza in modo unico in prodotto di elementi primi. Si dimostra poi che i domini principali, cioè i domini in cui ogni ideale è principale, hanno questa proprietà. Si studiano i domini euclidei, in cui vale una legge di divisione con resto, come in $\mathbb{Z}$. I domini euclidei risultano principali. Viene inoltre data la dimostrazione che l'anello degli interi di Gauss è un dominio euclideo.

Nel capitolo 12 si studiano i campi e le estensioni dei campi in relazione al problema generale della soluzione delle equazioni polinomiali. L'esempio motivante è dato dall'estensione $\mathbb{C}$ di $\mathbb{R}$ ottenuta mediante l'aggiunta della soluzione i dell'equazione $x^2 + 1 = 0$. Descriviamo le estensioni algebriche semplici, i campi di spezzamento di un polinomio e introduciamo i campi algebricamente chiusi. In particolare, viene dimostrato il teorema fondamentale dell'algebra. Studiamo inoltre alcuni polinomi notevoli e i polinomi sui campi finiti.

L'ultimo capitolo contiene oltre 300 suggerimenti e svolgimenti degli esercizi.

1

Insiemi, relazioni e funzioni

Nel primo e nel secondo paragrafo si introducono il concetto di insieme e di appartenenza e le operazioni tra insiemi. Nei paragrafi 3 e 4 si definiscono le relazioni su insiemi e le applicazioni. I paragrafi 6 e 7 sono dedicati alla distinzione tra insiemi finiti e infiniti e in particolare ai numeri naturali ed il principio di induzione. I paragrafi 8, 9 e 10 trattano le relazioni di equivalenza, i coefficienti binomiali e le relazioni d'ordine e preordine. Il paragrafo 11 è dedicato all'assioma della scelta e al lemma di Zorn, mentre il paragrafo 12 ai prodotti cartesiani. Infine il paragrafo 13 tratta l'equipotenza di insiemi ed i numeri cardinali. Questi ultimi paragrafi possono essere tralasciati da chi non fosse interessato ad una trattazione rigorosa dell'argomento.

1.1 Il concetto di insieme e di appartenenza

I concetti di insieme e appartenenza "$\in$" sono primitivi e non verranno definiti rigorosamente. Un insieme X è determinato dai suoi elementi x; scriveremo $x \in X$ e leggeremo *x appartiene a X*. Scriveremo spesso anche $X = \{x : \text{vale } P(x)\}$, dove $P(x)$ è qualche proprietà che descrive gli elementi di X. Nel caso in cui X abbia come elementi $x_1, x_2, \ldots, x_n$ scriveremo $X = \{x_1, x_2, \ldots, x_n\}$, cioè X è determinato dalla lista dei suoi elementi; è importante ribadire che questi elementi sono a due a due distinti.

Vediamo qualche esempio.

(a) L'insieme di tutti gli studenti dell'Università di Udine.
(b) L'insieme di tutte le rette del piano.
(c) L'insieme delle lettere dell'alfabeto latino.
(d) L'insieme dei colori dell'arcobaleno.

Vediamo ora qualche esempio numerico.

Esempio 1.1. (a) L'insieme $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$ dei numeri naturali.
(b) L'insieme $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$ dei numeri interi.

(c) L'insieme $\mathbb{Q}$ dei numeri razionali.
(d) L'insieme $\mathbb{R}$ dei numeri reali.
(e) L'insieme $\mathbb{N}_+ = \{x \in \mathbb{N} : x > 0\}$ dei numeri naturali positivi.
(f) L'insieme $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$ dei numeri reali positivi.
(g) L'insieme dei numeri primi $\mathbb{P} = \{2, 3, 5, \ldots\}$.

Esempio 1.2. (a) L'insieme $\{0, 2, 4, \ldots\}$ dei numeri naturali pari si può scrivere anche così:

$$\{x \in \mathbb{N} : x = 2y \text{ per qualche } y \in \mathbb{N}\}.$$

(b) L'intervallo aperto $]a, b[= \{x \in \mathbb{R} : a < x < b\}$ di estremi a e b in $\mathbb{R}$.
(c) L'intervallo chiuso $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ di estremi a e b in $\mathbb{R}$. Inoltre

$$[a, b[= \{x \in \mathbb{R} : a \leq x < b\}, \qquad]a, b] = \{x \in \mathbb{R} : a < x \leq b\},$$

$$]-\infty, b] = \{x \in \mathbb{R} : x \leq b\}, \qquad]-\infty, b[= \{x \in \mathbb{R} : x < b\},$$

$$[a, +\infty[= \{x \in \mathbb{R} : x \geq a\}, \qquad]a, +\infty[= \{x \in \mathbb{R} : x > a\}.$$

Essendo ogni insieme completamente determinato dai suoi elementi, due insiemi X e Y coincidono, cioè $X = Y$, se e solo se hanno gli stessi elementi. In altre parole per ogni $x \in X$ vale anche $x \in Y$ e per ogni $y \in Y$ vale anche $y \in X$. Se per due insiemi X ed Y è verificata solamente la prima delle implicazioni, cioè per ogni $x \in X$ vale anche $x \in Y$, diremo che X è *sottoinsieme* di Y o che X è una *parte* di Y o ancora che X è *contenuto* in Y, e verrà indicato con

$$X \subseteq Y.$$

In questa circostanza diremo anche Y *contiene* X e verrà indicato con

$$Y \supseteq X.$$

Valgono simultaneamente $X \subseteq Y$ e $Y \subseteq X$ se e solo se $X = Y$. Se invece vale $X \subseteq Y$, ma non vale $X = Y$, diremo che X è *sottoinsieme proprio* di Y e lo indicheremo con $X \subset Y$ o $Y \supset X$.

La condizione $x \notin \emptyset$ per ogni x determina un insieme $\emptyset$, privo di elementi, che chiameremo *l'insieme vuoto*. Vale $\emptyset \subseteq X$ per ogni insieme X: infatti basta trovare una proprietà P tale che nessun elemento di X soddisfa P. Per esempio:

$$\emptyset = \{x \in \mathbb{N} : 2x = 5\}, \qquad \emptyset = \{x \in \mathbb{Q} : x^2 = 2\},$$

$$\emptyset = \{x \in \mathbb{R} : x^4 = -11\}, \qquad \emptyset = \{x \in X : x \neq x\}.$$

Gli elementi di un insieme possono avere natura del tutto arbitraria. In particolare, possono essere insiemi essi stessi. Per esempio, se X ed Y sono insiemi, possiamo considerare l'insieme $Z = \{X, Y\}$, che ha come elementi X e Y. Se abbiamo n insiemi $A_1, \ldots, A_n$, possiamo considerare l'insieme $Z = \{A_1, \ldots, A_n\}$. Spesso ci riferiamo a Z dicendo anche "Z è una *famiglia* di insiemi" ("famiglia" e "insieme" sono sinonimi, la sfumatura serve solo per facilitare la comprensione). Ecco un esempio di una famiglia infinita di insiemi.

Esempio 1.3. Per ogni $x \in \mathbb{R}$ sia A_x l'intervallo $]x, x+1[$ in $\mathbb{R}$. Allora gli insiemi A_x, al variare di x in $\mathbb{R}$ formano una famiglia infinita di insiemi, che denoteremo con $\{A_x : x \in \mathbb{R}\}$.

Analogamente quando si ha una famiglia di insiemi A_i, indiciata con gli elementi i di un insieme di indici I, scriveremo $\{A_i : i \in I\}$.

Dato un insieme X consideriamo la famiglia $\mathcal{P}(X)$ di tutte le parti o sottoinsiemi di X. Questa famiglia si chiama *l'insieme delle parti* di X. Si noti che $\mathcal{P}(\emptyset)$ non è vuoto, essendo $\mathcal{P}(\emptyset) = \{\emptyset\}$. Si veda inoltre che $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. Se un sottoinsieme $\{x\}$ di un insieme X contiene un solo elemento si dice *singoletto*.

1.2 Operazioni tra gli insiemi

Siano X ed Y due insiemi. L'*unione* di X e Y è l'insieme $X \cup Y$ che ha come elementi tutti gli x tali che valga $x \in X$ *oppure* $x \in Y$. In altre parole,

$$X \cup Y = \{x : x \in X \text{ o } x \in Y\}.$$

Non è difficile vedere che

$$X \subseteq X \cup Y \text{ e } Y \subseteq X \cup Y. \tag{1}$$

L'unione $X \cup Y$ è il più piccolo insieme che soddisfa la proprietà (1). Infatti se Z soddisfa (1), cioè se $X \subseteq Z$ e $Y \subseteq Z$, allora anche $X \cup Y \subseteq Z$: se $x \in X \cup Y$, allora si ha $x \in X$ o $x \in Y$ e in entrambi casi segue $x \in Z$.

Si vede analogamente che l'operazione unione gode delle seguenti proprietà:

(1) $X \cup Y = Y \cup X$ per ogni coppia di insiemi X e Y (commutatività);
(2) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ per ogni terna di insiemi X, Y e Z (associatività);
(3) $A \cup A = A$ per ogni insieme A (idempotenza).

L'*intersezione* di due insiemi X e Y è l'insieme $X \cap Y$ che ha come elementi tutti gli x tali che vale $x \in X$ *e* $x \in Y$. In altre parole,

$$X \cap Y = \{x : x \in X \text{ e } x \in Y\}.$$

Per esempio, l'insieme $\mathbb{N}_+ = \{x \in \mathbb{N} : x > 0\}$ dei numeri naturali positivi si può vedere come l'intersezione $\mathbb{R}_+ \cap \mathbb{N}$.

Possiamo descrivere l'intersezione anche come

$$X \cap Y = \{x \in X : x \in Y\} = \{x \in Y : x \in X\}.$$

Due insiemi X ed Y si dicono *disgiunti* se $X \cap Y = \emptyset$.

Non è difficile vedere che $X \cap Y \subseteq X$ e $X \cap Y \subseteq Y$ e $X \cap Y$ è il più grande insieme che soddisfa tale proprietà, si veda l'esercizio 1.3.

L'operazione intersezione gode delle seguenti proprietà:

(1) $X \cap Y = Y \cap X$ per ogni coppia di insiemi X e Y (commutatività);
(2) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$ per ogni terna di insiemi X, Y e Z (associatività);
(3) $A \cap A = A$ per ogni insieme A (idempotenza).

Definiamo l'unione di una famiglia arbitraria di insiemi $\mathcal{F}$ ponendo

$$\bigcup_{A \in \mathcal{F}} A = \{x : x \in A \text{ per qualche } A \in \mathcal{F}\}.$$

Vediamo un esempio.

Esempio 1.4. L'insieme dei numeri reali $\mathbb{R}$ si può vedere come un'unione (infinita) di suoi intervalli

$$\mathbb{R} = \bigcup_{x \in \mathbb{Z}}]x, x+2[.$$

Questa uguaglianza resta vera se gli intervalli $]x, x+2[$ di lunghezza 2 vengono sostituiti con gli intervalli $]x, x+1[$ di lunghezza 1?

Come nel caso dell'unione, si può definire l'intersezione di una famiglia arbitraria $\mathcal{F}$ di insiemi, ponendo

$$\bigcap_{A \in \mathcal{F}} A = \{x : x \in A \text{ per ogni } A \in \mathcal{F}\}.$$

Alcuni esempi di intersezioni infinite si possono vedere negli esercizi 2.1 e 2.2.

Verifichiamo ora le *leggi distributive* dell'intersezione rispetto all'unione e dell'unione rispetto all'intersezione.

Proposizione 1.5. *Siano A, B e C tre insiemi, allora valgono:*

(a) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$;
(b) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

DIMOSTRAZIONE. (a) Sia $x \in (A \cap B) \cup C$, allora o $x \in A \cap B$ oppure $x \in C$, cioè o $x \in A$ e $x \in B$ oppure $x \in C$. Se x appartiene ad A e a B, allora $x \in A \cup C$ e $x \in B \cup C$. Se $x \in C$, allora $x \in A \cup C$ e $x \in B \cup C$. Pertanto in ogni caso $x \in (A \cup C) \cap (B \cup C)$.

Supponiamo ora $x \in (A \cup C) \cap (B \cup C)$. Allora $x \in A \cup C$ e $x \in B \cup C$. Se x non appartiene a C, allora da $x \in A \cup C$ si ricava che $x \in A$ e da $x \in B \cup C$ si ricava che x deve stare anche in B. Quindi o $x \in C$ oppure $x \in A \cap B$, cioè $x \in (A \cap B) \cup C$.

(b) Si prova in modo analogo ad (a). □

Definizione 1.6. Una famiglia $\{A : A \in \mathcal{F}\}$ di sottoinsiemi non vuoti A di un insieme X è una *partizione di X* se

(a) $X = \bigcup_{A \in \mathcal{F}} A$,
(b) $A \cap B = \emptyset$ se $A, B \in \mathcal{F}$ e $A \neq B$.

Vediamo qualche esempio.

Esempio 1.7. (a) Sia X un insieme. Allora $\{\{x\} : x \in X\}$ è una partizione di X.
(b) Consideriamo i seguenti tre insiemi
$X = \{$studenti dell'Università di Udine$\}$,
$F = \{$facoltà presenti presso l'Università di Udine$\}$ e
$X_f = \{$studenti iscritti alla facoltà $f \in F\}$.
Allora $\{X_f : f \in F\}$ è una partizione di X.
(c) L'insieme $\{[n, n+1[: n \in \mathbb{Z}\}$ è una partizione di $\mathbb{R}$.

La *differenza* di due insiemi X e Y, detta anche *complementare di* Y *in* X è l'insieme $X \setminus Y$ che ha come elementi tutti gli $x \in X$ tali che $x \notin Y$. In altre parole

$$X \setminus Y = \{x : x \in X \text{ e } x \notin Y\}. \tag{2}$$

Esempio 1.8. (a) Il complementare di $\mathbb{Q}$ in $\mathbb{R}$ è l'insieme dei numeri irrazionali.
(b) Il complementare dei numeri pari in $\mathbb{N}$ è l'insieme dei numeri dispari.
(c) Il complementare dei numeri dispari nell'insieme dei numeri primi $\mathbb{P}$ è $\{2\}$.

È facile vedere che $X \setminus X = \emptyset$ per ogni insieme X. Più precisamente, si ha:

Lemma 1.9. *Siano X ed Y insiemi. Allora $X \setminus Y = \emptyset$ se e solo se $X \subseteq Y$.*

DIMOSTRAZIONE. Sia $X \setminus Y = \emptyset$. Se $x \in X$, allora non possiamo avere $x \notin Y$, altrimenti $x \in X \setminus Y$ contrariamente all'ipotesi $X \setminus Y = \emptyset$. Questo dimostra l'inclusione $X \subseteq Y$.

Viceversa, se $X \subseteq Y$, allora non esiste un elemento $x \in X$ tale che $x \notin Y$. Pertanto la proprietà (2) definisce l'insieme vuoto. □

Vediamo ora alcune proprietà della differenza.

Proposizione 1.10. (Leggi di de Morgan) *Siano X un insieme, $A \in \mathcal{P}(X)$ e $\mathcal{F}$ un sottoinsieme di $\mathcal{P}(X)$. Allora*

(a) $A \setminus \bigcap_{B \in \mathcal{F}} B = \bigcup_{B \in \mathcal{F}} (A \setminus B)$;
(b) $A \setminus \bigcup_{B \in \mathcal{F}} B = \bigcap_{B \in \mathcal{F}} (A \setminus B)$.

DIMOSTRAZIONE. (a) Se $x \in A \setminus \bigcap_{B \in \mathcal{F}} B$, allora $x \in A$ ed esiste $B_0 \in \mathcal{F}$ tale che $x \notin B_0$. Pertanto $x \in A \setminus B_0$ e quindi a maggior ragione $x \in \bigcup_{B \in \mathcal{F}} (A \setminus B)$. Supponiamo viceversa $x \in \bigcup_{B \in \mathcal{F}} (A \setminus B)$, allora esiste B_0 tale che $x \in A \setminus B_0$. Pertanto $x \notin B_0$ e quindi $x \notin \bigcap_{B \in \mathcal{F}} B$, cioè $x \in A \setminus \bigcap_{B \in \mathcal{F}} B$.

(b) La dimostrazione è analoga. □

Introduciamo ora il prodotto cartesiano di due insiemi. Siano X ed Y due insiemi non vuoti. Per un elemento $x \in X$ e un elemento $y \in Y$ l'insieme $\{\{x\}, \{x, y\}\}$ si dice *coppia ordinata con prima coordinata x e seconda coordinata y* e si denota con (x, y). Non è difficile vedere che due coppie (x, y) e (x_1, y_1) coincidono se e solo se $x = x_1$ e $y = y_1$. Il *prodotto cartesiano* $X \times Y$ di X per Y è l'insieme di tutte le coppie ordinate (x, y), dove $x \in X$ e $y \in Y$.

Nel caso $X = Y$ l'insieme di tutte le coppie (x, x) con $x \in X$ si denota con Δ_X e si chiama *diagonale* di $X \times X$. Scriveremo X^2 per denotare $X \times X$.

Il prodotto cartesiano di più di due insiemi sarà introdotto e discusso nel paragrafo 1.12.

1.3 Relazioni e funzioni

In questo paragrafo introduciamo la definizione di relazione e studiamo vari tipi di relazioni binarie che godono di certe proprietà.

Definizione 1.11. Siano X ed Y insiemi non vuoti. Una *relazione binaria* di X in Y è un sottoinsieme R di $X \times Y$. Si dice una relazione binaria su X, se $X = Y$.

Un primo importantissimo esempio di relazione binaria è l'*applicazione*. La definizione intuitiva di applicazione è nata nell'ambito degli insiemi di numeri, o altri oggetti concreti, dove la "regola" di "calcolare" $f(x)$ a partire da x può avere senso.

Intuitivamente, un'*applicazione* $f : X \to Y$ tra due insiemi X ed Y è una regola che permette di assegnare ad *ogni* elemento $x \in X$ un *unico* elemento $f(x)$ di Y. Le due parole evidenziate sono le parole chiave per definire poi rigorosamente un'applicazione tra due insiemi. Notiamo ad esempio che la posizione $f : \mathbb{R} \to \mathbb{R}$ definita da $f(x) = \log x$ non è un'applicazione perché non è definita su ogni elemento di $\mathbb{R}$.

Esempio 1.12. (a) Sia $X = \{$studenti dell'Università di Udine$\}$, allora $f : X \to \mathbb{N}$ che associa ad ogni studente il suo numero di matricola, è un'applicazione.
(b) Se $X = \{$rette del piano$\}$, allora $f : X \to \mathbb{R} \cup \{\infty\}$ che associa ad ogni retta il suo coefficiente angolare rispetto ad un assegnato sistema di riferimento è un'applicazione.
(c) Esempi importanti di applicazioni sono le funzioni numeriche:
  (c_1) la funzione quadrato $f : \mathbb{R} \to \mathbb{R}$ definita da $f(x) = x^2$;
  (c_2) la funzione logaritmica $f : \mathbb{R}_+ \to \mathbb{R}$ definita da $f(x) = \log x$;
  (c_3) la funzione radice quadrata $f : \mathbb{R}_+ \to \mathbb{R}_+$ definita da $f(x) = \sqrt{x}$.

Vediamo ora alcuni esempi nel caso generale.

Esempio 1.13. (a) Sia X un insieme non vuoto. L'applicazione $id_X : X \to X$ definita dalla regola $id_X(x) = x$ per ogni $x \in X$ si dice *identità* o *applicazione identica* di X.
(b) Sia Y una parte non vuota di un insieme X.
  (b_1) L'applicazione $\iota_Y : Y \to X$ definita da $\iota_Y(x) = x$ per ogni $x \in Y$ si dice *immersione* di Y in X.
  (b_2) Sia $f : X \to Z$ un'applicazione. L'applicazione $f \restriction_Y : Y \to Z$ definita da $f \restriction_Y (y) = f(y)$ per ogni $y \in Y$ si dice *restrizione* di f ad Y.
(c) Sia X un insieme non vuoto. Allora $f : X \to \mathcal{P}(X)$ definita da $f(x) = \{x\}$ è un'applicazione.

Il *grafico* $G(f)$ di un'applicazione $f : X \to Y$ si definisce come l'insieme di tutte le coppie $(x, f(x)) \in X \times Y$ con $x \in X$, cioè

$$G(f) = \{(x,y) \in X \times Y : y = f(x)\}.$$

Ad esempio il grafico della funzione $f : \mathbb{R} \to \mathbb{R}$ del punto (c_1) dell'esempio 1.12 è la parabola $\{(x,y) \in \mathbb{R}^2 : y = x^2\}$ nel piano $\mathbb{R}^2$, mentre il grafico dell'applicazione identica $id_X : X \to X$ è la diagonale Δ_X di $X \times X$.

Non è difficile verificare che il grafico $G(f)$ è un sottoinsieme del prodotto cartesiano $X \times Y$ con le seguenti proprietà:

(A1) per ogni $x \in X$, esiste una coppia $(x,y) \in G(f)$;
(A2) se $(x,y) \in G(f)$ e $(x,y') \in G(f)$, allora $y = y'$.

1.4 Definizione rigorosa di applicazione

Proponiamo ora una definizione astratta di funzione, basata sulle proprietà (A1) e (A2) del grafico $G(f)$ di un'applicazione, descritte nel paragrafo precedente.

Definizione 1.14. Siano X ed Y insiemi non vuoti. Un'*applicazione* $f : X \to Y$ è un sottoinsieme G del prodotto cartesiano $X \times Y$, cioè una relazione con le proprietà:

(A1) per ogni $x \in X$, esiste una coppia $(x,y) \in G$;
(A2) se $(x,y) \in G$ e $(x,y') \in G$, allora $y = y'$.

L'insieme X si dice *dominio* dell'applicazione f e l'insieme Y si dice *codominio* dell'applicazione f. Si noti che ogni applicazione, nel senso della definizione 1.14, determina una "regola" che permette di "calcolare" $f(x) \in Y$ come l'unico elemento $y \in Y$ tale che $(x,y) \in G$.

Per $A \subseteq X$ l'insieme $f(A) = \{f(a) : a \in A\}$ è l'*immagine* di A. Se $a \in X$, $f(a) = f(\{a\})$ si chiama *immagine di a secondo f* o *valore di f in a*. L'insieme $f(X)$ di tutte le immagini degli elementi di X si chiama *immagine dell'applicazione f*.

Per $b \in Y$ l'insieme $\{x \in X : f(x) = b\}$ si chiama *immagine inversa di b* o *antimmagine di b* e si denota con $f^{-1}(b)$. Chiaramente $f^{-1}(b) \neq \emptyset$ se e solo se $b \in f(X)$. Per $B \subseteq Y$ l'insieme $\{x \in X : f(x) \in B\}$ si chiama *immagine inversa di B* e si denota con $f^{-1}(B)$.

Definizione 1.15. Siano X, Y due insiemi non vuoti. L'insieme di tutte le funzioni da X in Y si denota con $Y^X = \{f : X \to Y,\ f \text{ applicazione}\}$.

La seguente definizione introduce tre proprietà molto importanti delle applicazioni.

Definizione 1.16. Un'applicazione $f : X \to Y$ si dice:

(a) *iniettiva*, se per ogni $x, y \in X$ l'uguaglianza $f(x) = f(y)$ implica $x = y$; f si dice anche *iniezione*;

(b) *suriettiva*, se per ogni $y \in Y$ esiste $x \in X$ tale che $f(x) = y$; f si dice anche *suriezione*;
(c) *biettiva*, se f è iniettiva e suriettiva; f si dice anche *biezione*.

Osserviamo che $f : X \to Y$ è iniettiva se e solo se elementi distinti di X hanno immagini distinte in Y. In altre parole, f è iniettiva se e solo se $f^{-1}(b)$ contiene al più un elemento per ogni $b \in Y$. D'altra parte, f è suriettiva se e solo se $f(X) = Y$.

Esempio 1.17. Sia X un insieme non vuoto.

(a) L'applicazione id_X è iniettiva e suriettiva, quindi biettiva.
(b) Se Y è una parte non vuota di un insieme X, allora l'immersione $\iota_Y : Y \to X$ è iniettiva; ι è suriettiva se e solo se $Y = X$.

Teorema 1.18. (Teorema di Cantor) *Sia X un insieme non vuoto; non esiste un'applicazione suriettiva $f : X \to \mathcal{P}(X)$.*

DIMOSTRAZIONE. Supponiamo che esista un'applicazione $f : X \to \mathcal{P}(X)$ suriettiva. Sia $A = \{x \in X : x \notin f(x)\}$. Allora per la suriettività di f esiste $x_0 \in X$ con $f(x_0) = A$. Proviamo che per x_0 e A non valgono né $x_0 \in A$, né $x_0 \notin A$. Infatti, se $x_0 \in A$, allora $x_0 \notin f(x_0)$ per la definizione di A, assurdo. Se $x_0 \notin A$, allora $x_0 \in f(x_0) = A$, assurdo. □

Vogliamo sottolineare il ruolo importante delle applicazioni rispetto agli insiemi. A questo scopo faremo vedere come, a partire dalla nozione di applicazione, si possano definire:

(a) l'insieme delle parti $\mathcal{P}(X)$;
(b) le relazioni binarie;
(c) i prodotti cartesiani;
(d) i numeri naturali;
(e) gli insiemi finiti/infiniti.

Possiamo definire una biezione tra l'insieme delle parti $\mathcal{P}(X)$ e l'insieme $\{0,1\}^X$ di tutte le funzioni $X \to \{0,1\}$, tale insieme si denota brevemente anche con 2^X. Per $A \in \mathcal{P}(X)$ consideriamo la *funzione caratteristica* $\chi_A : X \to \{0,1\}$

$$\chi_A(x) = \begin{cases} 1 \text{ se } x \in A, \\ 0 \text{ se } x \in X, x \notin A. \end{cases}$$

Allora definiamo $\varphi(A) = \chi_A$. Si vede facilmente nell'esercizio 1.54, che φ è una biezione che permette di identificare $\mathcal{P}(X)$ con l'insieme 2^X delle funzioni caratteristiche.

Le relazioni binarie si possono definire tramite le applicazioni, facendo uso di (a). Sia $R \subseteq X \times X$ una relazione su X. Allora se consideriamo l'applicazione $\chi_R : X \times X \to \{0,1\}$ possiamo affermare che per $x, y \in X$ si ha xRy se e solo se $\chi_R(x,y) = 1$. In altre parole, la relazione R si può "codificare" tramite un'applicazione $X \times X \to \{0,1\}$.

I numeri naturali saranno introdotti nel paragrafo 1.6 tramite gli assiomi di Peano basati su un'applicazione specifica. Nel paragrafo 1.7 vedremo come la distinzione tra insiemi finiti/infiniti si possa fare esclusivamente tramite applicazioni.

Nel paragrafo 1.11 verrà introdotto un ordine buono su un'insieme X, a partire da un'applicazione $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ con la proprietà $f(A) \in A$ per ogni $A \in \mathcal{P}(X) \setminus \{\emptyset\}$.

Nel paragrafo 1.12 si useranno le applicazioni allo scopo di definire in modo efficace i prodotti cartesiani anche di famiglie infinite di insiemi.

Infine vedremo nel quarto capitolo come il concetto primario dell'algebra, l'**operazione binaria** su un insieme A, non sia altro che un'applicazione $A \times A \to A$.

1.5 Composizione di applicazioni

Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni tali che il dominio di g coincide con il codominio di f. La *composizione* di f e g è l'applicazione $g \circ f : X \to Z$ definita da $(g \circ f)(x) = g(f(x))$ per ogni $x \in X$. La composizione $g \circ f$ è detta spesso anche *applicazione composta* o *applicazione prodotto* di f e g.

Esempio 1.19. Sia Y una parte non vuota di un insieme X e sia $f : X \to Z$ un'applicazione. Allora la restrizione $f \restriction_Y$ coincide con la composizione dell'immersione $\iota_Y : Y \to X$ e f.

Proviamo che la composizione di applicazioni soddisfa la *legge associativa.*

Lemma 1.20. *Siano* $f : X \to Y$, $g : Y \to Z$ *ed* $h : Z \to W$ *tre applicazioni. Allora* $f \circ (g \circ h) = (f \circ g) \circ h$.

DIMOSTRAZIONE. Per verificare che queste due applicazioni coincidono basta verificare che per ogni $x \in X$ risulta:

$$(f \circ (g \circ h))(x) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x).$$

□

Consideriamo ora un caso in cui la composizione è sempre possibile.

Esempio 1.21. Sia X un insieme non vuoto. Allora la composizione $g \circ f$ è definita per ogni coppia di applicazioni f, g di X in se stesso. In particolare è definita la composizione $f \circ f$ che denoteremo nel seguito con f^2. Analogamente sono definite le composizioni $f \circ (f \circ f)$ e $(f \circ f) \circ f$ che coincidono per il lemma 1.20 e saranno denotate nel seguito con f^3. Una definizione più generale si trova nell'esempio 1.33.

La composizione di applicazioni preserva la proprietà di essere iniettiva o suriettiva.

Lemma 1.22. *Siano* $f : X \to Y$ *e* $g : Y \to Z$ *due applicazioni:*

(a) se f e g sono suriettive, allora anche $g \circ f$ è suriettiva;
(b) se f e g sono iniettive, allora anche $g \circ f$ è iniettiva.

DIMOSTRAZIONE. (a) Per dimostrare la suriettività di $g \circ f$, prendiamo un elemento $z \in Z$ del codominio e dimostriamo che esiste $x \in X$ tale che $g(f(x)) = z$. Poiché g è suriettiva, esiste $y \in Y$ tale che $g(y) = z$. Inoltre poiché f è suriettiva, esiste $x \in X$ tale che $y = f(x)$. Pertanto sostituendo y nella precedente uguaglianza, otteniamo proprio $z = g(y) = g(f(x))$, cioè $z = (g \circ f)(x)$.

(b) Per dimostrare che $g \circ f$ è iniettiva, supponiamo $(g \circ f)(x) = (g \circ f)(y)$ per qualche $x, y \in X$ e mostriamo che allora $x = y$. Dal fatto che g è iniettiva e che $g(f(x)) = g(f(y))$, otteniamo $f(x) = f(y)$. Dal fatto che pure f è iniettiva, otteniamo ora $x = y$. □

Possiamo parzialmente invertire questo risultato. In generale non è vero che se $g \circ f$ è iniettiva o suriettiva allora anche g ed f lo sono. Infatti:

Esempio 1.23. Sia $X = \mathbb{R} \setminus \{0\}$ e sia $f : X \to X$ definita da $f(x) = x^2$. Sia ora $g : X \to \mathbb{R}$ definita da $g(y) = \log(|y|)$. Allora $g \circ f$ è suriettiva, ma f non è suriettiva.

Esempio 1.24. Sia $f = \iota_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ l'immersione e sia $g : \mathbb{Z} \to \mathbb{Z}$ la funzione $g(x) = x^2$. Allora $g \circ f$ è iniettiva, mentre g non lo è.

Vediamo quindi come possiamo invertire il lemma 1.22.

Lemma 1.25. *Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni.*

(a) se $g \circ f$ è suriettiva, allora anche g è suriettiva;
(b) se $g \circ f$ è iniettiva, allora anche f è iniettiva.

DIMOSTRAZIONE. (a) Se $g \circ f$ è suriettiva, per ogni $z \in Z$ esiste $x \in X$ tale che $(g \circ f)(x) = g(f(x)) = z$. Sia dunque $y = f(x)$, allora $g(y) = g(f(x)) = z$. Questo dimostra che g è suriettiva.

(b) Siano $x, y \in X$ tali che $f(x) = f(y)$. Allora

$$(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y).$$

Dall'iniettività di $g \circ f$ otteniamo $x = y$. □

Il seguente esempio mostra come data un'applicazione iniettiva $f : X \to Y$ sia sempre possibile costruire, a partire da essa, un'applicazione suriettiva $g : Y \to X$.

Esempio 1.26. Se un'applicazione $f : X \to Y$ è iniettiva, allora esiste un'applicazione $g : Y \to X$ tale che $g \circ f = id_X$. Infatti fissiamo un elemento arbitrario $x_0 \in X$. Se $y \in f(X)$, poniamo $g(y) = x$, dove x è l'unico elemento di X con $f(x) = y$; se $y \in Y \setminus f(X)$ poniamo $g(y) = x_0$. Allora $g \circ f = id_X$. Notiamo che ogni applicazione g con questa proprietà è necessariamente suriettiva.

Per dimostrare che, data un'applicazione suriettiva $f : X \to Y$ è sempre possibile costruire un'applicazione iniettiva g con $f \circ g = id_Y$ è invece necessario l'Assioma della Scelta, come illustreremo nel paragrafo 1.11.

Proveremo ora che le applicazioni suriettive e quelle iniettive si possono caratterizzare tramite opportune proprietà di "cancellazione". Rendiamo il concetto preciso tramite la seguente definizione.

Definizione 1.27. Un'applicazione $f : X \to Y$ si dice

(a) *cancellabile a destra*, se $g_1 \circ f = g_2 \circ f$ implica $g_1 = g_2$ per ogni coppia di applicazioni $g_1, g_2 : Y \to Z$;
(b) *cancellabile a sinistra*, se $f \circ g_1 = f \circ g_2$ implica $g_1 = g_2$ per ogni coppia di applicazioni $g_1, g_2 : Z \to X$.

Teorema 1.28. *Sia $f : X \to Y$ un'applicazione. Allora:*

(a) f è cancellabile a destra se e solo se f è suriettiva;
(b) f è cancellabile a sinistra se e solo se f è iniettiva.

DIMOSTRAZIONE. (a) Supponiamo che f sia suriettiva. Per provare che f è cancellabile a destra consideriamo una coppia di applicazioni $g, h : Y \to Z$ con $g \circ f = h \circ f$. Per vedere che $g = h$ scegliamo $y \in Y$ e notiamo che $y = f(x)$ per qualche $x \in X$. Ma allora $g(y) = (g \circ f)(x) = (h \circ f)(x) = h(y)$. Quindi $g = h$. Se invece f non è suriettiva, esiste $y_0 \in Y \setminus f(X)$. Fissiamo un elemento $y_1 \in f(X)$. Poniamo $g = id_Y$ e consideriamo l'applicazione $h : Y \to Y$ definita da

$$h(y) = \begin{cases} y, & \text{se } y \in f(X) \\ y_1, & \text{se } y \in Y \setminus f(X) \end{cases}$$

Allora $g(y_0) = y_0 \neq y_1 = h(y_0)$, da cui $g \neq h$ nonostante valga $g \circ f = h \circ f$. Quindi f non è cancellabile a destra.

(b) Supponiamo che f sia iniettiva. Per provare che f è cancellabile a sinistra consideriamo una coppia di applicazioni $g, h : Z \to X$ con $f \circ g = f \circ h$. Sia $z \in Z$. Allora $f \circ g = f \circ h$ implica $f(g(z)) = f(h(z))$. Quindi $g(z) = h(z)$ e $g = h$. Supponiamo che f non sia iniettiva. Allora $f(x) = f(y)$ per due elementi distinti $x \neq y$ in X. Sia $Z = \{z\}$ un singoletto arbitrario. Allora le applicazioni $g, h : Z \to X$, definite da $g(z) = x$ e $h(z) = y$, sono distinte. Tuttavia $f \circ g = f \circ h$ e quindi f non è cancellabile a sinistra. □

Definizione 1.29. Un'applicazione $f : X \to Y$ si dice *invertibile*, se esiste un'applicazione $g : Y \to X$ tale che $g \circ f = id_X$ e $f \circ g = id_Y$, cioè $g(f(x)) = x$ per ogni $x \in X$ e $f(g(y)) = y$ per ogni $y \in Y$. Una tale applicazione si dice *inversa di* f.

Diamo una caratterizzazione delle applicazioni invertibili.

Teorema 1.30. *Un'applicazione $f : X \to Y$ è invertibile se e solo se è biettiva. In tal caso l'inversa di f è unica.*

DIMOSTRAZIONE. Supponiamo che l'applicazione f sia biettiva. Per ogni $y \in Y$, esiste $x \in X$ tale che $f(x) = y$, poiché f è suriettiva. Inoltre tale x è unico perché f è anche iniettiva. Poniamo $g(y) = x$. Si ha $f(g(y)) = f(x) = y$, per ogni $y \in Y$ per la definizione di g. D'altra parte, per ogni $x \in X$ si ha $g(f(x)) = x$ sempre per la definizione di g. Pertanto $f \circ g = id_Y$ e $g \circ f = id_X$, quindi g è l'inversa di f.

Proviamo che se f è invertibile, allora f è biettiva e l'inversa di f è unica. Per ipotesi esiste un'applicazione $g : Y \to X$ tale che $g \circ f = id_X$ e $f \circ g = id_Y$. Per l'esempio 1.17, $g \circ f$ è iniettiva, quindi per (b) del lemma 1.25 concludiamo che f è iniettiva. Analogamente, l'esempio 1.17 garantisce che $f \circ g$ sia suriettiva, quindi per (a) del lemma 1.25 concludiamo che f è suriettiva. Essendo iniettiva e suriettiva, f risulta biettiva. Se g' fosse un'altra inversa di f, allora da $g \circ f = id_X = g' \circ f$ e dal teorema 1.28 dedurremo $g = g'$ poiché f è suriettiva. □

Nel seguito denoteremo con f^{-1} l'unica inversa di un'applicazione invertibile f.

Un'applicazione $f : X \to X$ si dice *involutoria* o semplicemente, una *involuzione* se $f \circ f = id_X$. Ogni applicazione involutoria è invertibile con $f^{-1} = f$ e pertanto biettiva.

Le applicazioni biettive $X \to X$ di un insieme X si dicono anche *permutazioni* di X.

1.6 I numeri naturali e il principio di induzione

L'insieme $\mathbb{N} = \{0, 1, 2, \ldots\}$ dei *numeri naturali* è uno dei concetti primitivi la cui esistenza non può essere provata. Il matematico italiano Peano (1858-1932) propose la seguente descrizione assiomatica.

Assiomi di Peano. Esiste un insieme N e un applicazione $s : N \to N$, detta *successore*, tale che

(P1) $a \in N$;
(P2) se $n \in N$, allora anche $s(n) \in N$;
(P3) se $n \in N$, allora $s(n) \neq a$;
(P4) s è iniettiva;
(P5) se l'insieme E contiene a ed ha la proprietà che assieme ad ogni $n \in E$ anche $s(n) \in E$, allora $N \subseteq E$.

Osserviamo che l'elemento a che non appartiene all'immagine $s(N)$ è univocamente determinato. Infatti sia $E = s(N) \cup \{a\}$, allora E soddisfa la proprietà (P5) e quindi $E = N$, da cui si deduce $\{a\} = N \setminus s(N)$.

Come tutti gli assiomi, anche gli assiomi di Peano non possono essere dimostrati. O meglio si possono dimostrare, supponendo però che valga un altro assioma, cioè l'esistenza di un insieme infinito nel senso di Cantor, come mostreremo nel teorema 1.41. Sarà importante il fatto che s sia iniettiva (P4), ma non suriettiva (P3).

Proviamo nell'esercizio 1.16 che se (N_1, s_1) e (N_2, s_2) sono due insiemi che soddisfano gli assiomi di Peano, allora esiste una biezione $f : N_1 \to N_2$ compatibile con le applicazioni s_1 e s_2 nel modo seguente: se

$$\{a_1\} = N_1 \setminus s_1(N_1) \text{ e } \{a_2\} = N_2 \setminus s_2(N_2),$$

si ha $f(a_1) = a_2$ e $f(s_1(n)) = s_2(f(n))$ per ogni $n \in N_1$.

Un'applicazione con questa proprietà si dice un'*isomorfismo di sistemi di Peano* e rende le due coppie (N_1, s_1) e (N_2, s_2) praticamente indistinguibili. D'ora in avanti denotiamo con $\mathbb{N}$ un insieme soddisfacente gli assiomi di Peano, con 0 l'unico elemento definito da (P1), con 1 l'unico elemento $s(0)$, con 2 l'unico elemento $s(1)$, $3 = s(2)$ e così via, denotando con $n + 1$ l'unico elemento $s(n)$ per ogni elemento $n \in \mathbb{N}$. Chiamiamo $\mathbb{N}$ l'insieme dei *numeri naturali*.

Se $m = s(n)$, diremo che m è *successore* di n, mentre diremo che n è *predecessore* di m e lo denoteremo con $n = m - 1$.

Osserviamo che ad eccezione degli assiomi (P1) e (P2) che enfatizzano il fatto di avere un'applicazione $s : N \to N$, gli assiomi di Peano non sono "ridondanti", cioè nessuno di essi è dimostrabile a partire dagli altri. Lo si può verificare esibendo delle terne (N, a, s) dove solo uno degli assiomi di Peano non venga soddisfatto e N non sia isomorfo come sistema di Peano all'insieme dei numeri naturali. Diamo un suggerimento di come si possano costruire questi insiemi.

Se eliminiamo (P3), si può considerare $N = \{0, 1\}$ con $s : N \to N$ definita da $s(0) = 1$ e $s(1) = 0$.

Se eliminiamo (P4), sia di nuovo $N = \{0, 1\}$, $s(0) = s(1) = 1$, allora i restanti quattro assiomi sono soddisfatti.

Infine se eliminiamo (P5), possiamo considerare l'insieme $N = \mathbb{N}$ con $a = 0$, ed $s(n) = (n + 1) + 1$.

Dedichiamo ora la nostra attenzione interamente all'assioma (P5) che è senz'altro la più importante proprietà dei numeri naturali, nota anche come *principio di induzione*, perciò la riformuliamo separatamente.

Proposizione 1.31. *Supponiamo che S sia un sottoinsieme di $\mathbb{N}$ tale che $0 \in S$ e per ogni $x \in S$ si ha che anche $s(x) \in S$. Allora $S = \mathbb{N}$.*

Il principio di induzione dà luogo ad una tecnica molto usata in matematica, le cosiddette "dimostrazioni per induzione", di cui daremo diverse forme, nelle proposizioni 1.32, 1.59 e 1.58.

Proposizione 1.32. (Principio di induzione - prima forma) *Per ogni $n \in \mathbb{N}$, consideriamo un'asserzione $A(n)$ e supponiamo che*

(a) $A(0)$ sia vera;

(b) se $A(k)$ è vera per $k \in \mathbb{N}$, allora anche $A(k + 1)$ è vera.

Allora l'asserzione $A(n)$ è vera per ogni $n \in \mathbb{N}$.

DIMOSTRAZIONE. Sia S l'insieme degli $n \in \mathbb{N}$ per i quali $A(n)$ è vera. Allora $0 \in S$ e da $n \in S$ segue $n + 1 \in S$. Quindi $S = \mathbb{N}$ per il principio di induzione 1.31. □

Il principio di induzione è fondamentale non solo per le dimostrazioni per induzione, ma anche per le *definizioni* per induzione. Se vogliamo definire un oggetto $D(n)$ per ogni $n \in \mathbb{N}$, basta definire l'oggetto $D(0)$ e per ogni $k \in \mathbb{N}$

per il quale è stato già definito $D(k)$, definire anche $D(k+1)$. Il principio di induzione garantisce che $D(n)$ è stato definito per ogni $n \in \mathbb{N}$. Infatti l'insieme $E = \{n \in \mathbb{N} : f(n) \text{ è definito}\}$ contiene 0 e $n \in E$ implica $n+1 \in E$.

Esempio 1.33. (a) Per un insieme non vuoto X ed un'applicazione $f : X \to X$ definiamo rigorosamente le *potenze* f^n per tutti gli $n \in \mathbb{N}$. Poniamo $f^0 = id_X$ e se f^n è già definito per $n \in \mathbb{N}$, poniamo $f^{n+1} = f \circ f^n$.

(b) In particolare, per $X = \mathbb{N}$ e l'applicazione successore $s : \mathbb{N} \to \mathbb{N}$, si hanno le potenze s^n per tutti gli $n \in \mathbb{N}$. Per esempio, $s^2(0) = 2, s^3(0) = 3, \ldots$. In altre parole, $s^n(0) = n$ per ogni $n \in \mathbb{N}$. Analogamente $s^2(1) = 3, s^3(1) = 4, \ldots$, cioè $s^n(1) = n+1$ per $n \in \mathbb{N}$. Lasciamo la facile prova per induzione al lettore.

Possiamo definire la somma $m+n$ per due numeri naturali $m, n \in \mathbb{N}$ come

$$m + n = s^n(m).$$

Oppure, fissando m arbitrariamente in $\mathbb{N}$, possiamo definire la somma $D(n) = m+n$ anche direttamente: poniamo $D(0) = m$ e supponendo di aver già definito $D(n)$, poniamo $D(n+1) = D(n) + 1$.

Per $m, n \in \mathbb{N}$, poniamo $m \leq n$, se $n = m + k$ per qualche $k \in \mathbb{N}$ e scriviamo $k = n - m$. Nel caso $m \leq n$ e $m \neq n$, scriviamo $m < n$. Così risulta

$$0 < 1 < 2 < 3 < 4 < \ldots < n < n+1 < \ldots$$

Un'ultima osservazione sul principio di induzione: nelle proposizioni 1.32 e 1.59 si può sostituire nelle ipotesi $A(0)$ con $A(n_0)$, per qualche $n_0 \in \mathbb{N}$ e la tesi sarà quindi *$A(n)$ è vera per ogni $n \geq n_0$, $n \in \mathbb{N}$.*

Dimostriamo che la somma $+$ in $\mathbb{N}$ soddisfa la legge commutativa e la legge associativa.

Lemma 1.34. *Per tutti gli $m, n, k \in \mathbb{N}$ valgono le proprietà*

(a) $(m+n)+k = m+(n+k)$ *(associativa);*
(b) $m+n = n+m$ *(commutativa);*
(c) se $m+n = k+n$, *allora* $m = k$.

DIMOSTRAZIONE. (a) Ragioniamo per induzione su k con $m, n \in \mathbb{N}$ fissati arbitrariamente. L'asserto è vero per $k = 0$, mentre l'uguaglianza

$$(m+n)+1 = m+(n+1) \text{ per tutti gli } m, n \in \mathbb{N} \tag{3}$$

segue immediatamente dalla definizione della somma. Supponiamo per ipotesi induttiva di avere $(m+n)+k = m+(n+k)$ per qualche $k \in \mathbb{N}$. Allora $((m+n)+k)+1 = (m+(n+k))+1$. Applicando (3) ad ambo i membri dell'equazione, ricaviamo $(m+n)+(k+1) = m+((n+k)+1) = m+(n+(k+1))$. Questo prova (a).

(b) Dimostriamo prima che $s^n \circ s = s \circ s^n$ per ogni $n \in \mathbb{N}$. L'asserto è banalmente vero per $n = 0$. Supponiamo che $s^n \circ s = s \circ s^n$ per qualche $n \in \mathbb{N}$. Allora per il lemma 1.20 si ha $s \circ s^{n+1} = s \circ (s \circ s^n) = s \circ (s^n \circ s) = (s \circ s^n) \circ s = s^{n+1} \circ s$.

Per dimostrare l'uguaglianza $m + n = n + m$ per tutti gli $m, n \in \mathbb{N}$ ragioniamo per induzione su m, e lo dimostriamo per ogni $n \in \mathbb{N}$ fissato. Per $m = 0$ si ha

$$0 + n = s^n(0) = n = n + 0.$$

Supponiamo di avere $m + n = n + m$ per qualche $m \in \mathbb{N}$. Ora applicando $s^n \circ s = s \circ s^n$ ad m si ha $(m + 1) + n = (m + n) + 1$. Quindi

$$(m + 1) + n = (m + n) + 1 = (n + m) + 1 = n + (m + 1).$$

Questo dimostra $m + n = n + m$ per tutti gli $m, n \in \mathbb{N}$.

(c) Basta osservare che $s^n(m) = m + n = k + n = s^n(k)$, e che s^n è iniettiva, in quanto composta di iniettive. □

La legge associativa permette di definire somme di tre numeri naturali $m + n + k$ come $(m + n) + k = m + (m + k)$. Analogamente si può definire la somma

$$a_1 + a_2 + \ldots + a_n \text{ di } n > 2 \text{ numeri naturali.}$$

Nel seguito denoteremo questa somma brevemente con

$$\sum_{k=1}^{n} a_k,$$

dove l'indice k varia da 1 a n e può essere sostituito da qualunque altro carattere, per esempio $\sum_{i=1}^{n} a_i$ o $\sum_{j=1}^{n} a_j$.

Diamo ora altre due importanti definizioni per induzione. Definiamo il prodotto $\cdot$ di due numeri naturali $n, m \in \mathbb{N}$, ponendo per ogni $n \in \mathbb{N}$:

$0 \cdot n = 0$;
$1 \cdot n = n$;
$m \cdot n = (m - 1) \cdot n + n$, per $m \geq 2$.

Nel seguito ometteremo il segno $\cdot$ cioè scriveremo mn per indicare $m \cdot n$. Osserviamo che se $m \neq 0$ e $n \neq 0$, allora $mn \geq n > 0$, da cui segue $mn = 0$ se e solo se $m = 0$ o $n = 0$. Questo dimostra (d) del seguente lemma. Lasciamo per esercizio la dimostrazione dei punti (a), (b) e (c).

Lemma 1.35. *Per tutti gli $m, n, k \in \mathbb{N}$ valgono le seguenti proprietà*

(a) $(mn)k = m(nk)$ *(associativa);*
(b) $mn = nm$ *(commutativa);*
(c) $m(n + k) = mn + mk$ *(distributiva rispetto alla somma);*
(d) $mn = 0$ *se e solo se* $m = 0$ *o* $n = 0$.

Il lemma ci permette di definire m^n per ogni numero naturale $m > 0$ e $n \in \mathbb{N}$ come segue: $m^0 = 1$, e $m^n = m^{n-1}m$, se $n > 0$.

Il punto (d) del lemma si ricava facilmente anche dalla seguente proprietà più generale che si può dimostrare per induzione: $mn = kn$ per tre numeri naturali m, n e k con $n > 0$ se e solo se $m = k$.

Un numero naturale n si dice *pari*, se $n = 2m$ per qualche $m \in \mathbb{N}$, altrimenti si dice che n è *dispari*. Si dimostra facilmente per induzione che ogni numero dispari n si può presentare nella forma $n = 2m + 1$ per qualche $m \in \mathbb{N}$. Una proprietà più precisa dei numeri naturali si può trovare nell'esercizio 1.17.

Per ogni numero naturale, definiamo infine il *fattoriale*.

Definizione 1.36. Sia $n \in \mathbb{N}$, definiamo $n!$ come segue:
$0! = 1$;
$n! = n \cdot (n-1)!$ per $n \geq 1$.

Osserviamo che $1! = 1$ e $n! = 1 \cdot 2 \cdot \ldots \cdot n$ per $n \geq 2$.

1.7 Insiemi finiti e infiniti

Un insieme X è *finito*, se X è vuoto o esistono un numero naturale $n > 0$ e una biezione $f : \{1, 2, \ldots, n\} \to X$. Diremo in tal caso che X ha cardinalità n e scriveremo $|X| = n$, ponendo per completezza $|\emptyset| = 0$. Se $x_k = f(k)$ per $k = 1, 2, \ldots, n$, scriveremo anche $X = \{x_1, x_2, \ldots, x_n\}$. Se X è finito ed esiste una biezione $X \to Y$, allora anche Y è finito e $|Y| = |X|$. In particolare, si potrebbe usare anche l'insieme $\{0, 1, \ldots, n-1\}$ per decidere se $|X| = n$.

Proviamo che sottoinsiemi e immagini di insiemi finiti sono ancora finiti.

Lemma 1.37. *Sia X un insieme finito.*

(a) Se $Y \subseteq X$, allora Y è un insieme finito e $|Y| \leq |X|$.
(b) Se $f : X \to Z$ è un'applicazione suriettiva, anche Z è finito.

DIMOSTRAZIONE. (a) Supponiamo che X sia un insieme finito, con $n = |X|$. Per dimostrare che $Y \subseteq X$ è finito, ragioniamo per induzione su n. I casi $n = 0$ e $n = 1$ sono ovvi. Supponiamo $n > 1$ e l'asserto vero per n. Sia ora X un insieme finito con $|X| = n + 1$ e sia $Y \subseteq X$. Non è restrittivo pensare $X = \{1, \ldots, n+1\}$. Se $Y = \emptyset$, allora $|Y| = 0$. Supponiamo pertanto $Y \neq \emptyset$ e poniamo

$$Y_1 = Y \cap \{1, \ldots, n\} \quad \text{e} \quad Y_2 = Y \cap \{n+1\}; \quad \text{si ha} \quad Y = Y_1 \cup Y_2.$$

Ora Y_1 è finito per l'ipotesi induttiva e quindi esiste una biezione $f : \{1, \ldots, m\} \to Y_1$, per qualche $m \in \mathbb{N}$. Distinguiamo due casi. Se $Y_2 = \emptyset$, allora $Y = Y_1$ e abbiamo concluso. Altrimenti $Y_2 = \{n+1\}$ è finito. Sia $g : \{1, \ldots, m, m+1\} \to Y$ definita da $g(i) = f(i)$, se $i = 1, \ldots, m$ e $g(m+1) = n+1$. Allora g è una biezione e pertanto Y è finito. Inoltre vale $|Y| \leq |X|$.

(b) Consideriamo l'applicazione suriettiva $f : X \to Z$ e per ogni $z \in Z$ scegliamo $y \in X$ tale che $f(y) = z$. Sia Y l'insieme di tali y al variare di z in Z. Allora la restrizione di f ad Y è una biezione. Essendo Y finito per la prima parte del lemma, concludiamo che anche Z è finito. □

Utilizzando il lemma 1.37, si ha $X \cap Y$ finito, se X ed Y sono finiti. Una facile induzione permette poi di dimostrare che anche $X \cup Y$ è finito, si veda l'esercizio

1.28. Più precisamente, se X e Y sono anche disgiunti, allora $|X \cup Y| = |X| + |Y|$. Inoltre anche il prodotto cartesiano $X \times Y$ è finito e vale $|X \times Y| = |X| \times |Y|$, come si dimostra nell'esercizio 1.57. Infine, se X è finito, anche $\mathcal{P}(X)$ è finito e $|\mathcal{P}(X)| = 2^{|X|}$, si veda l'esercizio 1.55.

Proviamo un teorema molto utile sugli insiemi finiti.

Teorema 1.38. (Principio di Dirichlet) *Se X e Y sono insiemi finiti con $|X| > |Y|$, allora non esiste alcuna iniezione $X \to Y$.*

DIMOSTRAZIONE. Siano $n = |X|$ e $m = |Y|$. Senza ledere la generalità, possiamo supporre $X = \{1, 2, \dots, n\}$ e $Y = \{1, 2, \dots, m\}$. Inoltre

$$m < n \implies m + 1 \leq n.$$

Essendo la restrizione di un'iniezione sempre un iniezione, possiamo supporre $X = \{1, 2, \dots, m+1\}$. Dunque, basta dimostrare per induzione su m che non esiste un'iniezione di $X = \{1, 2, \dots, m+1\}$ in $Y = \{1, 2, \dots, m\}$. Per $m = 1$ l'asserto è vero. Supponiamo che sia vero per qualche $m \in \mathbb{N}$ e supponiamo per assurdo che esista un'iniezione f di

$$X = \{1, 2, \dots, m+2\} \quad \text{in} \quad Y = \{1, 2, \dots, m+1\}.$$

Se $m + 1 \notin f(X)$, troviamo un'iniezione $\{1, 2, \dots, m+2\} \to \{1, 2, \dots, m\}$ che ristretta ad $\{1, 2, \dots, m+1\}$ contraddice l'ipotesi induttiva. Pertanto esiste $k \in X$ tale che $f(k) = m + 1$. Sia $g : X \to X$ l'applicazione definita da

$$g(x) = \begin{cases} x, \text{ se } x \in X \text{ e } x \neq k, m+2, \\ m+2, \text{ se } x = k \\ k, \text{ se } x = m+2 \end{cases}$$

Allora g è biettiva e $h = f \circ g : X \to Y$ è un'iniezione con $h(m+2) = m+1$. Pertanto la restrizione $h\restriction_{\{1,2,\dots,m+1\}}$ è un'iniezione tra $\{1, 2, \dots, m+1\}$ e $\{1, 2, \dots, m\}$, assurdo. □

Dirichlet usava formulare questo principio nel modo seguente: *se disponiamo m oggetti in n scatole e $m > n$, allora almeno una scatola conterrà non meno di due oggetti.* Per un'applicazione di questo principio, si veda anche l'esercizio 2.3.

Dal principio di Dirichlet si ricava facilmente il seguente corollario.

Corollario 1.39. *Ogni iniezione $X \to X$ di un insieme finito X è anche una suriezione.*

DIMOSTRAZIONE. Sia $f : X \to X$ un'iniezione. Allora $Y = f(X)$ è un sottoinsieme finito di X, f fornisce una biezione $X \to Y$ e quindi $|Y| = |X|$. Essendo $X = Y \cup (X \setminus Y)$ una partizione, vale $|X| = |Y| + |X \setminus Y|$ per l'esercizio 1.28. Pertanto $|X \setminus Y| = 0$ e di conseguenza $X \setminus Y = \emptyset$. Quindi $Y = X$ e f è suriettiva.
□

Abbiamo visto che tutte le operazioni tra gli insiemi finiti danno come risultato sempre un insieme finito. Per ottenere degli insiemi infiniti è quindi necessario introdurre qualche assioma, o gli assiomi di Peano o un assioma che garantisca l'esistenza di un insieme infinito nel senso di Cantor, come vedremo nel teorema 1.41. Nel seguito ci occuperemo di insiemi infiniti. È naturale dire che un insieme X è *infinito*, se X non è finito. Dal principio di Dirichlet si ricava immediatamente che $\mathbb{N}$ è infinito. Infatti se per assurdo $\mathbb{N}$ fosse finito, esisterebbe una biezione $f : \mathbb{N} \to \{1, 2, \dots, n\}$, e restringendo f all'insieme $\{1, 2, \dots, n+1\}$, otterremmo un'iniezione, contraddicendo il principio di Dirichlet 1.38. Riassumiamo tre diverse definizioni di infinito che si possono dare. Mostreremo nel teorema 1.42 che in effetti queste tre definizioni sono equivalenti.

Definizione 1.40. Un insieme X è *infinito*, se X non è finito.

Un insieme X è *infinito nel senso di Dedekind*, se esiste una iniezione $\mathbb{N} \to X$.

Un insieme X è *infinito nel senso di Cantor*, se esiste un'applicazione iniettiva, ma non suriettiva $f : X \to X$.

Il concetto di insieme infinito nel senso di Dedekind presume l'esistenza di $\mathbb{N}$, mentre quello proposto da Cantor non fa ricorso alcuno ai numeri naturali.

Nel paragrafo 1.6 è stata introdotta la funzione iniettiva successore s che non è suriettiva, quindi l'insieme $\mathbb{N}$ è infinito nel senso di Cantor. Dimostriamo ora che l'esistenza di un qualunque insieme infinito nel senso di Cantor permette di costruire una coppia (C, s) che soddisfa gli assiomi di Peano e quindi, per l'esercizio 1.16, l'insieme dei numeri naturali $\mathbb{N}$.

Teorema 1.41. *Sia X un insieme infinito nel senso di Cantor. Allora esistono un sottoinsieme C di X e un'applicazione iniettiva $s : C \to C$ tali che la coppia (C, s) soddisfa gli assiomi di Peano.*

DIMOSTRAZIONE. Per ipotesi esiste un'applicazione iniettiva, ma non suriettiva $f : X \to X$. Sia $x \in X \setminus f(X)$. Sia $\mathcal{A}$ la famiglia di tutti i sottoinsiemi A di X contenenti x e tali che $f(A) \subseteq A$. Allora $\mathcal{A}$ è non vuota, poiché $X \in \mathcal{A}$. L'insieme $C = \bigcap_{A \in \mathcal{A}} A$ soddisfa $f(C) \subseteq C$, essendo ovviamente $f(C) \subseteq A$ per ogni $A \in \mathcal{A}$. Quindi $C \in \mathcal{A}$ in quanto $x \in C$. Pertanto C è il più piccolo elemento di $\mathcal{A}$. Sia $s : C \to C$ la restrizione di f a C. Allora C, s soddisfano (P1) e (P2) degli assiomi di Peano e, poiché s è iniettiva, anche (P4). Osserviamo che $x \notin s(C)$ perché $x \notin f(X)$, per cui vale (P3). Per vedere che vale (P5) si noti che ogni insieme $E \subseteq C$ con la proprietà $x \in E$ e $s(E) \subseteq E$ necessariamente appartiene ad $\mathcal{A}$ in quanto $f(E) = s(E)$. Quindi $E = C$ per le proprietà di C di essere il più piccolo elemento di $\mathcal{A}$. Dunque la coppia (C, s) soddisfa gli assiomi di Peano. □

Il teorema 1.41 implica, in particolare, che ogni insieme X infinito nel senso di Cantor è infinito anche nel senso di Dedekind, si veda anche l'esercizio 1.30. Riassumiamo tutto ciò che abbiamo visto sugli insiemi infiniti nel seguente teorema, mostrando che le tre definizioni di insieme infinito sono equivalenti.

Teorema 1.42. *Per un insieme X le seguenti tre proprietà sono equivalenti:*

(a) X è infinito;
(b) X è infinito nel senso di Cantor;
(c) X è infinito nel senso di Dedekind.

DIMOSTRAZIONE. (b) $\Rightarrow$ (c) Se X è infinito nel senso di Cantor, X è infinito nel senso di Dedekind per il teorema 1.41.

(c) $\Rightarrow$ (b) Supponiamo che esista un'applicazione iniettiva $h : \mathbb{N} \to X$. Allora possiamo scrivere $X = h(\mathbb{N}) \cup Y$, dove $Y = X \setminus h(\mathbb{N})$. Sia $s : \mathbb{N} \to \mathbb{N}$ l'applicazione definita da $s(n) = n + 1$. Allora l'applicazione $f : X \to X$, che coincide con $h \circ s \circ h^{-1}$ su $h(\mathbb{N})$ ed è l'identità su Y, è iniettiva, ma non suriettiva.

(b) $\Rightarrow$ (a) Dal corollario 1.39 ogni iniezione $X \to X$ di un insieme finito X è anche una suriezione. Quindi gli insiemi infiniti nel senso di Cantor risultano infiniti.

(a) $\Rightarrow$ (c) Proviamo che gli insiemi infiniti risultano infiniti anche nel senso di Dedekind.

Per ipotesi non esiste alcuna biezione dall'insieme $\{1, 2, \ldots, n\}$ all'insieme X per alcun n e quindi non esiste una suriezione $\{1, 2, \ldots, n\} \to X$ per alcun n. Pertanto per ogni numero naturale $n > 0$ esistono almeno $n + 1$ elementi distinti di X. Possiamo costruire così un'iniezione $f : \mathbb{N} \to X$ nel modo seguente. Scegliamo un elemento arbitrario $x_0 \in X$ e poniamo $f(0) = x_0$. Supponiamo di aver già definito $f(0), \ldots, f(n-1)$. Poiché X ha un elemento x_n diverso da $f(0), \ldots, f(n-1)$ possiamo porre $f(n) = x_n$. Costruiamo in tal modo un'iniezione da $\mathbb{N}$ in X. □

Lemma 1.43. *Il numero di tutte le applicazioni iniettive di un insieme finito X con n elementi in un insieme Y con m elementi è uguale a $m \cdot (m-1) \cdot \ldots \cdot (m-n+1)$.*

DIMOSTRAZIONE. Prima di cominciare notiamo che l'asserto è banalmente vero per $m < n$, perché in tal caso non ci sono applicazioni iniettive di X in Y per il principio di Dirichlet, mentre il numero $m \cdot (m-1) \cdot \ldots \cdot (m-n+1)$ è uguale a 0 essendo il fattore $(m - m) = 0$. Pertanto assumeremo nel seguito che $m \geq n$.

Poiché X è un insieme finito, possiamo numerare i suoi elementi, cioè scrivere $X = \{x_1, x_2, \ldots, x_n\}$. Contiamo quali sono le possibili immagini di x_1 in Y tramite un'applicazione iniettiva. Possiamo scegliere tra tutti gli m elementi di Y. Ci sono pertanto m scelte. Ora l'immagine di x_2 può essere un qualsiasi elemento di Y, eccetto l'immagine di x_1, perché l'applicazione deve essere iniettiva. Pertanto si hanno $m - 1$ scelte per l'immagine di x_2. Proseguendo in questo modo, le possibili scelte per le immagini dell'elemento x_i, una volta scelte le immagini degli elementi x_j, $1 \leq j < i$, sono $m(m-1)(m-2)\ldots(m-i+1)$. Concludiamo con x_n, da cui segue l'enunciato. □

Dal lemma 1.43 si deduce il seguente corollario.

Corollario 1.44. *Sia X un insieme finito con n elementi. Allora il numero di tutte le permutazioni di X è $n! = 1 \cdot 2 \cdot \ldots \cdot n$.*

1.8 Relazioni di equivalenza

Introduciamo in questo paragrafo un particolare tipo di relazione.

Definizione 1.45. Una relazione binaria R su un insieme X si dice *relazione di equivalenza*, se sono verificate le seguenti proprietà:

(1) $(x,x) \in R$ per ogni $x \in X$ (riflessiva);
(2) $(x,y) \in R$ implica $(y,x) \in R$, per ogni coppia $x,y \in X$ (simmetrica);
(3) $(x,y) \in R$ e $(y,z) \in R$, implicano $(x,z) \in R$ per ogni terna $x,y,z \in X$ (transitiva).

Nel seguito scriveremo brevemente xRy al posto di $(x,y) \in R$.

Ad ogni relazione di equivalenza R sono associate le *classi di equivalenza* $[a]_R$, per $a \in X$, nel modo seguente:

$$[a]_R = \{x \in X : xRa\}.$$

Si noti che $a \in [a]_R$ per la proprietà (1), pertanto le classi $[a]_R$ sono non vuote. Se due classi di equivalenza $[a]_R$ e $[b]_R$ hanno elementi in comune, allora esse coincidono. Infatti, supponiamo che $[a]_R \cap [b]_R \neq \emptyset$ e fissiamo un elemento $z \in [a]_R \cap [b]_R$. Poiché ogni $x \in [a]_R$ soddisfa xRa, da $z \in [a]_R$ si ricava xRz per la transitività di R. Ora da xRz e zRb si ha analogamente xRb, quindi $x \in [b]_R$. Analogamente si dimostra che $[b]_R \subseteq [a]_R$. Quindi l'insieme delle classi di equivalenza risulta una partizione di X:

$$X = \bigcup_{a \in X} [a]_R.$$

Proviamo che questo risultato si può invertire.

Teorema 1.46. *Esiste una corrispondenza biunivoca tra le relazioni di equivalenza definite su un insieme X e le partizioni di X.*

DIMOSTRAZIONE. Abbiamo già dimostrato che ogni relazione di equivalenza su X definisce una partizione di X. Supponiamo ora di avere una partizione di X

$$\mathcal{L} = \{X_i : i \in I\}.$$

Definiamo una relazione di equivalenza $R_{\mathcal{L}}$ su X nel modo seguente: $xR_{\mathcal{L}}y$ se e solo se $x,y \in X_i$ per uno stesso insieme X_i di $\mathcal{L}$. Verifichiamo che tale relazione è di equivalenza:

-riflessiva: poiché $\mathcal{L}$ è una partizione, ogni elemento $x \in X$ appartiene a qualche X_i, $i \in I$, quindi $xR_{\mathcal{L}}x$.

-simmetrica: se $xR_{\mathcal{L}}y$, allora x,y appartengono allo stesso insieme X_i, pertanto vale anche $yR_{\mathcal{L}}x$.

-transitiva: se $xR_{\mathcal{L}}y$ e $yR_{\mathcal{L}}z$, allora $x,y \in X_i$ per qualche $i \in I$ e $y,z \in X_j$ per qualche $j \in I$. Poiché $\mathcal{L}$ è una partizione, avremo $X_i \cap X_j = \emptyset$ se $i \neq j$. Nel nostro caso $y \in X_i \cap X_j$, che non può pertanto essere vuota. Allora $i = j$ e $x,y,z \in X_i$, quindi $xR_{\mathcal{L}}z$.

Data una relazione di equivalenza R, si consideri la partizione in classi di equivalenza $\mathcal{L}_R = \{[a]_R : a \in X\}$ definita prima. Allora la relazione di equivalenza $R_{\mathcal{L}_R}$ costruita a partire da $\mathcal{L}_R$ coincide con R: infatti $aR_{\mathcal{L}_R}b$ se e solo se $a, b \in [a]_R$ se e solo se aRb. D'altra parte, per ogni partizione $\mathcal{L}$ di X la relazione di equivalenza $R_{\mathcal{L}}$ genera, tramite le sue classi di equivalenza, la partizione di partenza $\mathcal{L}$. Questo conclude la dimostrazione. □

Definizione 1.47. Sia R una relazione di equivalenza su un insieme non vuoto X. L'insieme delle classi di equivalenza $\{[x]_R : x \in X\}$ si dice *insieme quoziente di X modulo la relazione di equivalenza R* e si denota con X/R. L'applicazione $\pi : X \to X/R$ definita da $\pi(x) = [x]_R$ per ogni $x \in X$ di dice *applicazione canonica*. L'applicazione canonica è suriettiva.

Vediamo ora che ogni applicazione dà luogo ad una relazione di equivalenza nel suo dominio.

Esempio 1.48. Sia $f : X \to Y$ un'applicazione. Allora la relazione binaria R_f definita da

$$aR_fb \text{ se e solo se } f(a) = f(b)$$

è una relazione di equivalenza. Per ogni $y \in f(X)$, possiamo considerare

$$f^{-1}(y) = \{a \in X : f(a) = y\} = [a]_{R_f} \quad \text{per ogni } a \in f^{-1}(y).$$

Allora $\{f^{-1}(y) : y \in f(X)\}$ è una partizione di X.

Viceversa siano X un insieme non vuoto, R una relazione di equivalenza su X e $\overline{X} = X/R$ l'insieme quoziente. Se $\pi : X \to \overline{X}$ è l'applicazione canonica, allora R coincide con la relazione R_π.

Lo scopo del seguente teorema è di presentare un'applicazione arbitraria $f : X \to Y$ come composizione di due applicazioni delle quali la prima è suriettiva e la seconda è iniettiva.

Teorema 1.49. *Siano $f : X \to Y$ un'applicazione, $\overline{X} = X/R_f$ l'insieme quoziente modulo R_f e $\pi : X \to \overline{X}$ l'applicazione canonica. Allora esiste un'applicazione iniettiva $\overline{f} : \overline{X} \to Y$ tale che $f = \overline{f} \circ \pi$.*

DIMOSTRAZIONE. Definiamo $\overline{f} : \overline{X} \to Y$ con $\overline{f}([x]_{R_f}) = f(x)$. Mostriamo che $\overline{f}$ è ben definita e iniettiva.

$$[x]_{R_f} = [y]_{R_f} \iff f(x) = f(y) \iff \overline{f}([x]_{R_f}) = \overline{f}([y]_{R_f}).$$

Infine $(\overline{f} \circ \pi)(x) = \overline{f}(\pi(x)) = \overline{f}([x]_{R_f}) = f(x)$. □

1.9 Partizioni e coefficienti binomiali

Ci proponiamo di calcolare il numero di tutte le partizioni di un insieme X di n elementi. Per avere una visione più chiara della situazione vediamo ogni partizione di X come una colorazione di X, in altre parole vedremo le classi di equivalenza come "colori".

Il mondo in bianco e nero. Sia $n \geq 1$ un numero naturale e sia X un insieme di n elementi. Allora il numero di tutte le colorazioni di X in due colori, bianco e nero, è uguale a 2^n. Infatti ogni colorazione di X si potrebbe considerare come un'applicazione $\mathbf{c} : X \to \mathcal{C}$, dove $\mathcal{C}$ è l'insieme dei due colori $\{bianco, nero\}$ in modo da poter vedere il valore $\mathbf{c}(x)$ assunto in $x \in X$ come il colore (bianco o nero) di x. Notiamo che ogni colorazione $\mathbf{c}$ di X è completamente determinata dall'insieme

$$B_{\mathbf{c}} = \{x \in X : \mathbf{c}(x) = bianco\}$$

degli elementi bianchi di $\mathbf{c}$ poiché l'insieme

$$N_{\mathbf{c}} = \{x \in X : \mathbf{c}(x) = nero\}$$

degli elementi neri di $\mathbf{c}$ è precisamente il complemento $X \setminus B_{\mathbf{c}}$ di $B_{\mathbf{c}}$. Per chi preferisce vedere il mondo in nero, aggiungiamo che anche l'insieme $N_{\mathbf{c}}$ determina completamente la colorazione $\mathbf{c}$. Inoltre le colorazioni costanti sono le due colorazioni monocolore:

(a) $\mathbf{b} : X \to \mathcal{C}$ con $B_{\mathbf{b}} = X$ e $N_{\mathbf{b}} = \emptyset$ (cioè tutto bianco);
(b) $\mathbf{n} : X \to \mathcal{C}$ con $N_{\mathbf{n}} = X$ e $B_{\mathbf{n}} = \emptyset$ (cioè tutto nero).

Le colorazioni suriettive sono quelle che hanno effettivamente tutti e due i colori, cioè non sono monocolori e sono quindi $2^n - 2$.

Osserviamo che ad ogni colorazione $\mathbf{c}$ in due colori corrisponde una partizione di X in due parti disgiunte $B_{\mathbf{c}}$ e $N_{\mathbf{c}}$, ma ad ogni partizione di X in due insiemi disgiunti Y e Z corrispondono *due* colorazioni di X che danno la partizione $X = Y \cup Z$. Per ogni k con $0 \leq k \leq n$, il numero delle colorazioni $\mathbf{c}$, con insieme "bianco" $B_{\mathbf{c}}$ consistente precisamente di k elementi, è uguale al numero delle k-uple non ordinate in X. Diamo un nome a questo numero.

Definizione 1.50. Il numero C_k^n è il numero delle k-uple non ordinate in un insieme di n elementi, si chiama *coefficiente binomiale di n rispetto a k* e si denota anche con

$$\binom{n}{k}.$$

Osserviamo che in particolare $C_0^n = C_n^n = 1$. Notiamo che se l'insieme "bianco" $B_{\mathbf{c}}$ ha k elementi, allora l'insieme "nero" $N_{\mathbf{c}}$ consiste di $n - k$ elementi. Analogamente il numero delle colorazioni $\mathbf{c}$, con insieme "nero" $N_{\mathbf{c}}$ di k elementi, è uguale

a C_k^n. Poiché le colorazioni con k elementi bianchi sono precisamente le colorazioni con $n-k$ elementi neri, si ricava immediatamente l'uguaglianza

$$C_k^n = C_{n-k}^n. \tag{4}$$

Dimostriamo una relazione tra i coefficienti binomiali, dalla quale possiamo calcolare esplicitamente C_k^n.

Lemma 1.51. *Siano $n, k \in \mathbb{N}$, $n \geq 1$ e $0 \leq k \leq n$. Allora valgono*

$$C_k^n = C_k^{n-1} + C_{k-1}^{n-1}, \quad se \quad k > 0 \tag{5}$$

$$C_k^n = \frac{n!}{k!(n-k)!} \tag{6}$$

DIMOSTRAZIONE. Sia X un insieme con n elementi. Contiamo le colorazioni con k elementi bianchi di X fissando un elemento $x_0 \in X$. Presentando X come $X' \cup \{x_0\}$, con X' il complemento di $\{x_0\}$ in X, osserviamo che ci sono C_k^{n-1} colorazioni di X con k elementi bianchi in X', cioè diversi da x_0 e C_{k-1}^{n-1} colorazioni con k elementi bianchi di cui uno è x_0. Infatti quest'ultime corrispondono alle colorazioni di X' con $k-1$ elementi bianchi. Questo prova (5).

Dimostriamo (6) per induzione su n, per ogni k con $0 \leq k \leq n$. Se $n = 1$, $C_0^1 = 1 = C_1^1$. Supponiamo che valga

$$C_k^{n-1} = \frac{(n-1)!}{k!(n-1-k)!} \quad \text{per ogni} \quad k \leq n-1.$$

Come già osservato, vale

$$C_0^n = C_n^n = 1 = \frac{n!}{n!0!},$$

quindi è sufficiente dimostrare la formula (6) per $0 < k < n$. Utilizziamo (5) e l'ipotesi induttiva

$$C_k^n = C_k^{n-1} + C_{k-1}^{n-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{n!}{k!(n-k)!}.$$

□

Il nome "coefficiente binomiale" proviene dalla seguente *formula del binomio*..

Lemma 1.52. *Dati a, b numeri reali, $n \in \mathbb{N}, n \geq 1$ vale*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{7}$$

DIMOSTRAZIONE. Lo dimostriamo per induzione su n. Il caso $n = 1$ è banale. Sia ora $n \geq 2$ e supponiamo la formula (7) vera per $n-1$. Allora

$$(a+b)^n = (a+b)^{n-1}(a+b) = \left(\sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-1-k}b^k\right)(a+b) =$$

$$= \sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-k}b^k + \sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-1-k}b^{k+1}.$$

Nell'ultima sommatoria sostituiamo $k+1$ all'indice k, ottenendo

$$\sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-k}b^k + \sum_{k=1}^{n}\binom{n-1}{k-1}a^{n-k}b^k =$$

$$= a^n + \sum_{k=1}^{n-1}\left(\binom{n-1}{k} + \binom{n-1}{k-1}\right)a^{n-k}b^k + b^n =$$

$$= a^n + \sum_{k=1}^{n-1}\binom{n}{k}a^{n-k}b^k + b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

La penultima uguaglianza si ottiene applicando (5). □

Ponendo in (7) $a = -b = 1$, si ottiene la seguente relazione tra i coefficienti binomiali

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0.$$

I coefficienti binomiali si possono disporre in un triangolo illimitato, noto come il *triangolo di Tartaglia–Pascal* dove (4) e (5) hanno un'interpretazione geometrica elegante:

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
. . . .

Il primo e l'ultimo coefficiente binomiale su ogni riga del triangolo sono uguali a 1. Inoltre il triangolo è simmetrico rispetto all'asse verticale e ogni coefficiente binomiale all'interno del triangolo è somma dei due coefficienti binomiali che gli stanno immediatamente sopra.

Abbiamo calcolato nel lemma 1.43 il numero

$$V_m^n = n(n-1)\dots(n-m+1)$$

di tutte le applicazioni iniettive di un insieme finito X con m elementi in un'insieme Y con n elementi e $m < n$. Si deduce immediatamente da (6) che

$$V_m^n = m! \cdot C_m^n.$$

Questa osservazione ci permette di trovare un'altra dimostrazione diretta della formula (6) che non fa uso di induzione. Infatti, poniamo $X = \{1, 2, \ldots, m\}$. Allora ad ogni m-upla fissata $B = \{y_1, y_2, \ldots, y_m\}$ di elementi distinti di Y corrisponde un'unica applicazione iniettiva $f : X \to Y$ con immagine B e $f(i) = y_i$ per $i = 1, 2, \ldots, m$. Quindi ad ogni sottoinsieme B di m elementi di Y corrispondono precisamente $m!$ applicazioni iniettive dell'insieme X in Y aventi come immagine questo sottoinsieme specifico di m elementi di X (per il fatto che ci sono $m!$ permutazioni degli elementi di B). Pertanto il numero C_m^n di tutti i sottoinsiemi distinti B di Y aventi m elementi risulta uguale a $V_m^n/m!$.

1.10 Relazioni di ordine e preordine

Una relazione binaria R in un insieme X si dice *relazione di preordine* se R è riflessiva e transitiva. Chiaramente ogni relazione di equivalenza è anche una relazione di preordine. Più precisamente, una relazione di preordine è una relazione di equivalenza se e solo se è anche simmetrica. Si può considerare invece la seguente proprietà detta *antisimmetrica*, di una relazione binaria R: $(x, y) \in R$ e $(y, x) \in R$ implicano $x = y$ per ogni coppia $x, y \in X$.

Definizione 1.53. Una relazione di preordine R in un insieme X si dice *relazione d'ordine* se R è anche antisimmetrica.

Per una relazione d'ordine si usa spesso anche il termine *ordine parziale*. Una relazione di (pre)ordine si denota solitamente con $\leq$, $\prec$ ecc. Un insieme dotato di una relazione d'ordine si dice un *insieme ordinato* e due elementi x, y di un insieme ordinato $(X, \leq)$ si dicono *confrontabili* se $x \leq y$ oppure $y \leq x$.

Esempio 1.54. Sia X un insieme non vuoto. Allora:

(a) la relazione $A \leq B$ in $\mathcal{P}(X)$ definita da $A \leq B$ se e solo se $A \subseteq B$ è una relazione di ordine;
(b) la relazione $A \preceq B$ in $\mathcal{P}(X)$ definita da $A \preceq B$ se e solo se $B \subseteq A$ è una relazione di ordine;
(c) la relazione $A \leq^* B$ in $\mathcal{P}(X)$ definita da

$$A \leq^* B \text{ se e solo se la differenza } B \setminus A \text{ è finita}$$

è una relazione di preordine.

Definizione 1.55. Sia $\leq$ un ordine su un insieme X, e Y un sottoinsieme non vuoto di X.

- l'ordine $\leq$ si dice *totale* o *lineare*, se ogni coppia di elementi x, y di X sono confrontabili;

- un elemento $y \in Y$ si dice *minimo di Y* se $y \leq z$ per ogni $z \in Y$; analogamente un elemento y di Y si dice *massimo di Y* se $y \geq z$ per ogni $z \in Y$;
- un elemento $y \in Y$ si dice *minimale di Y* se per ogni $z \in Y$ si ha che $z \leq y$ implica $y = z$; analogamente un elemento y di Y si dice *massimale di Y* se per ogni $z \in Y$ si ha che $y \leq z$ implica $y = z$;
- un elemento $y \in X$ si dice *minorante di Y* se per ogni $z \in Y$ si ha che $y \leq z$; analogamente un elemento y di X si dice *maggiorante di Y* se per ogni $z \in Y$ si ha che $z \leq y$;
- un elemento x di X si dice *estremo inferiore di Y in X* se x è il massimo dei minoranti di Y; analogamente un elemento x di X si dice *estremo superiore di Y in X* se x è il minimo dei maggioranti di Y;
- un sottoinsieme Y di X si dice *limitato superiormente* (rispettivamente *inferiormente*) se ammette *maggioranti* (rispettivamente minoranti);
- l'ordine $\leq$ si dice *completo*, se ogni sottoinsieme non vuoto e superiormente limitato di X ha estremo superiore e ogni sottoinsieme non vuoto e inferiormente limitato di X ha estremo inferiore;
- l'ordine $\leq$ si dice *denso* se dati $x, y \in X$, tali che $x < y$, esiste $z \in X$ tale che $x < z < y$;
- l'ordine $\leq$ si dice *buono* se ogni sottoinsieme non vuoto Y di X ha un elemento minimo.

Sia $(A, \leq)$ un insieme parzialmente ordinato. Un sottoinsieme C di A si dice una *catena* se $(C, \leq)$ è totalmente ordinato. Nel caso in cui C sia finita, la *lunghezza* della catena C è $|C|$.

Definizione 1.56. Un insieme ordinato $(L, \leq)$ si dice *reticolo* se per ogni coppia $a, b \in L$ l'insieme $\{a, b\}$ ammette estremo superiore, denotato con $a \vee b$, e estremo inferiore, denotato con $a \wedge b$. Il reticolo si denota con $(L, \wedge, \vee)$.

Se L ha anche elemento minimo e massimo, essi si denotano solitamente con 0 e 1, rispettivamente. In tal caso il reticolo si dice *limitato* e si denota con $(L, \wedge, \vee, 0, 1)$.

Ogni insieme totalmente ordinato è banalmente un reticolo.

Numerosi esempi di insiemi parzialmente ordinati e di reticoli si possono trovare negli esercizi 1.38, 1.45, 1.49, 1.52 e 1.53.

Esempio 1.57. Abbiamo definito la relazione $\leq$ sull'insieme $\mathbb{N}$ ponendo $x \leq y$ se esiste $n \in \mathbb{N}$ tale che $y = s^n(x) = x + n$. Tale relazione risulta un ordine. Notiamo che se $x < y$, allora $x + 1 \leq y$. Infatti $x < y$ implica $y = x + n$ con $n > 0$, quindi $y = (x + 1) + (n - 1)$ per la legge associativa. Dunque $x + 1 \leq y$.

Dal principio di induzione segue il fatto che questo è un buon ordinamento di $\mathbb{N}$. Data la sua importanza, riformuliamo questo fatto, noto anche come *principio del minimo* o *principio del buon ordinamento* e ne diamo una dimostrazione completa.

Proposizione 1.58. (Principio del buon ordinamento) *Ogni insieme non vuoto di numeri naturali possiede un elemento minimo.*

DIMOSTRAZIONE. Dimostriamo che $(\mathbb{N}, \leq)$ è totalmente ordinato. Proveremo per induzione che per ogni coppia $m, n \in \mathbb{N}$ vale $m \leq n$ o $n \leq m$. Fissiamo m arbitrariamente e facciamo induzione su n. Allora abbiamo ovviamente $m \geq 0$. Supponiamo di avere $m \leq n$ o $n \leq m$ per un certo $n \in \mathbb{N}$. Se vale $m \leq n$ vale anche $m \leq n + 1$. Se invece non vale $m \leq n$, per l'ipotesi induttiva deve valere $n < m$. Per l'esempio 1.57 possiamo concludere $n + 1 \leq m$. Abbiamo dimostrato che l'ordine $\leq$ è totale.

Sia E un insieme non vuoto di $\mathbb{N}$. Consideriamo l'insieme

$$E' = \{m \in \mathbb{N} : \text{ esiste } n \in E, n \leq m\}.$$

Allora

$$E \subseteq E' \quad \text{ e se } m \in E' \text{ e } m \leq l, \text{ allora anche } l \in E'. \tag{8}$$

Se m_0 fosse un elemento minimo per E', allora $m_0 \leq n$ per ogni $n \in E$. Inoltre esiste $n_0 \in E$ con $n_0 \leq m_0$. Pertanto $m_0 = n_0 \in E$ e quindi m_0 è un elemento minimo anche per E. Ci resta dunque da trovare un elemento minimo per E'. Sia $n_1 \in E'$. Se $n \notin E'$, allora $n < n_1$ per (8) e per il fatto che l'ordine $\leq$ è totale. Quindi il complemento Y di E' è finito, essendo contenuto nell'insieme finito $\{0, 1, 2, \ldots, n_1 - 1\}$ per il lemma 1.37. Per l'esercizio 1.42, Y ha un elemento massimale y. Allora $y + 1 \notin Y$, e quindi $y + 1 \in E'$. Dimostriamo che $y + 1$ è un elemento minimo di E'. Infatti per ogni $e \in E'$ non può valere $e \leq y$ poiché $y \notin E'$ per (8). Essendo l'ordine totale, dal fatto che e non soddisfa $e \leq y$, concludiamo che deve valere $y + 1 \leq e$ (si veda l'esempio 1.57). Poiché vale $y + 1 \leq e$ per tutti gli $e \in E'$, $y + 1$ risulta un elemento minimo di E' e di conseguenza anche di E. □

Possiamo ora provare anche il principio di induzione in un'altra forma.

Proposizione 1.59. (Principio di induzione - seconda forma) *Per ogni $n \in \mathbb{N}$, consideriamo un'asserzione $A(n)$ e supponiamo che*

(a) $A(0)$ sia vera;
(b) per ogni $m > 0$, se $A(k)$ è vera per ogni $0 \leq k < m$, allora anche $A(m)$ è vera.

Allora l'asserzione $A(n)$ è vera per ogni $n \in \mathbb{N}$.

DIMOSTRAZIONE. Sia S l'insieme degli $n \in \mathbb{N}$ per i quali $A(n)$ non è vera. Supponiamo per assurdo che S non sia vuoto, allora per il principio del minimo 1.58 esiste un elemento minimo m di S. Poiché per ipotesi $0 \notin S$, possiamo supporre $m > 0$. Inoltre per ogni $0 \leq k < m$, $A(k)$ è vera per la minimalità di m. Per ipotesi, questo implica $A(m)$ vera, contraddicendo $m \in S$. □

Diamo ora alcune regole di calcolo che possono essere utili nel seguito.

Lemma 1.60. *Sia $m \geq 2$ un numero naturale e sia assegnato un numero naturale $a_{k\nu}$ per ogni coppia k, ν con $2 \leq \nu \leq k \leq m$. Allora*

$$\sum_{k=2}^{m}\left(\sum_{\nu=2}^{k} a_{k\nu}\right) = \sum_{\nu=2}^{m}\left(\sum_{k=\nu}^{m} a_{k\nu}\right).$$

DIMOSTRAZIONE. Ragioniamo per induzione su m. Per $m = 2$ si ha

$$\nu = k = m = 2,$$

e quindi entrambe le somme coincidono con a_{22}. Supponiamo che valga

$$\sum_{k=2}^{m}\left(\sum_{\nu=2}^{k} a_{k\nu}\right) = \sum_{\nu=2}^{m}\left(\sum_{k=\nu}^{m} a_{k\nu}\right)$$

per qualche $m \geq 2$. Allora

$$\sum_{k=2}^{m+1}\left(\sum_{\nu=2}^{k} a_{k\nu}\right) = \sum_{k=2}^{m}\left(\sum_{\nu=2}^{k} a_{k\nu}\right) + \sum_{\nu=2}^{m+1} a_{m+1\,\nu} =$$

$$= \sum_{\nu=2}^{m}\left(\sum_{k=\nu}^{m} a_{k\nu}\right) + \sum_{\nu=2}^{m} a_{m+1\,\nu} + a_{m+1\,m+1} =$$

$$= \sum_{\nu=2}^{m}\left(\sum_{k=\nu}^{m} a_{k\nu} + a_{m+1\,\nu}\right) + a_{m+1\,m+1} = \sum_{\nu=2}^{m+1}\left(\sum_{k=\nu}^{m+1} a_{k\nu}\right).$$

□

Questa "regola di scambio" è molto utile quando ogni addendo è della forma $a_{k\nu} = c_\nu d_{k\nu}$ e la somma $S_\nu = \sum_{k=\nu}^{m} d_{k\nu}$ ha una forma semplice. In tal caso si avrà

$$\sum_{k=2}^{m}\left(\sum_{\nu=2}^{k} a_{k\nu}\right) = \sum_{\nu=2}^{m} c_\nu S_\nu.$$

Come si vede anche nell'esercizio 3.35, la seconda forma del principio di induzione è molto più flessibile della prima forma. Il seguente esempio evidenzia come si debba prestare attenzione nell'applicare il principio di induzione.

Esempio 1.61. Dimostriamo che tutti i cavalli sono bianchi. Basterà dimostrare che tutti cavalli sono dello stesso colore. Poiché tutti abbiamo visto almeno un cavallo bianco, la tesi segue immediatamente. Sia $A(n)$ l'affermazione "in ogni insieme di n cavalli tutti i cavalli sono dello stesso colore". Ovviamente $A(1)$ è vera. Siano $C_1, \ldots, C_n$ dei cavalli. Allora per l'ipotesi induttiva tutti i cavalli $C_1, \ldots, C_{n-1}$ sono dello stesso colore. Ora applichiamo l'ipotesi induttiva ai cavalli $C_2, C_3, \ldots, C_{n-1}, C_n$ e ne deduciamo che anch'essi sono dello stesso colore, che per forza deve essere il colore di C_{n-1}. Pertanto tutti i cavalli $C_1, \ldots, C_n$ sono dello stesso colore e quindi $A(n)$ è stata dimostrata.

Dov'è l'errore nell'esempio 1.61? Si veda l'esercizio 1.25.

1.11 Assioma della scelta

In questo paragrafo introduciamo un'assioma detto l'*assioma della scelta*, in quanto sarà poi necessario per poter introdurre i prodotti cartesiani infiniti di insiemi. Esso può essere formulato in varie forme equivalenti. Solitamente si usa la seguente.

Definizione 1.62. Sia $\{A_i\}_{i \in I}$ una famiglia di insiemi non vuoti con $I \neq \emptyset$. Un'applicazione $f : I \to \bigcup_{i \in I} A_i$ con la proprietà $f(i) \in A_i$ per ogni $i \in I$, si chiama *funzione di scelta* per la famiglia $\{A_i\}_{i \in I}$.

Assioma della scelta. *Ogni famiglia non vuota di insiemi non vuoti ammette una funzione di scelta.*

Nonostante l'apparente evidenza dell'esistenza della funzione di scelta, l'assioma della scelta non è dimostrabile a partire degli altri assiomi della teoria degli insiemi. Lo utilizziamo per dimostrare una proprietà delle applicazioni simile a quella già vista nell'esempio 1.26. Si può dimostrare che essa risulta un'altra forma equivalente dell'assioma della scelta.

Teorema 1.63. *Un applicazione $f : X \to Y$ è suriettiva se e solo se esiste un'applicazione $g : Y \to X$ tale che $f \circ g = id_Y$. Ogni applicazione g con questa proprietà è necessariamente iniettiva.*

DIMOSTRAZIONE. Sia $f : X \to Y$ un'applicazione suriettiva. Allora, dato $y \in Y$, esiste $x \in X$ tale che $f(x) = y$. Si scelga $x \in f^{-1}(y)$ e si definisca $g : Y \to X$ tramite $g(y) = x$. Per costruzione della g, si ha $f(g(y)) = f(x) = y$.

Se esiste un applicazione $g : Y \to X$ tale che $f \circ g = id_Y$, allora f è suriettiva perché la suriettività di $id_Y = f \circ g$ implica la suriettività di f. Analogamente l'iniettività di id_Y implica che g è iniettiva. □

Riassumendo, dal teorema 1.63 e dall'esempio 1.26 deduciamo che

Corollario 1.64. *Siano X, Y insiemi non vuoti. Allora esiste un applicazione suriettiva*

$$f : X \to Y$$

se e solo se esiste un applicazione iniettiva

$$g : X \to Y.$$

La seguente importante proprietà è nota come lemma di Zorn. Essa trova molte applicazioni nell'algebra e nell'analisi per dimostrare l'esistenza di certi oggetti con proprietà estremali. Lo utilizzeremo diverse volte nei capitoli successivi, ad esempio nei lemmi 1.80, 6.47 e nel teorema di Krull 9.33.

Per poter enunciare il lemma di Zorn, abbiamo prima bisogno di una definizione.

Definizione 1.65. Un insieme parzialmente ordinato $(A, \leq)$ si dice *induttivo* se ogni catena ha un maggiorante.

L'esercizio 1.35 garantisce l'esistenza di insiemi induttivi, per esempio tutti gli insiemi parzialmente ordinati finiti. In un insieme parzialmente ordinato $(X, \leq)$ possiamo definire per ogni $x \in X$, il *segmento iniziale di* x come l'insieme $I_X(x) = \{y \in X : y < x\}$.

Vedremo che la dimostrazione del lemma di Zorn usa l'assioma della scelta. D'altra parte, si può dimostrare che questo lemma implica l'assioma della scelta.

Lemma di Zorn. *Ogni insieme parzialmente ordinato e induttivo ammette elementi massimali.*

DIMOSTRAZIONE. Sia $(X, \leq)$ un insieme ordinato induttivo. Supponiamo per assurdo che X non abbia elementi massimali e denotiamo con $\mathcal{B}$ la famiglia di tutti i sottoinsiemi superiormente limitati di X. Per la nostra ipotesi, $X \notin \mathcal{B}$ e ogni catena di X è superiormente limitata, quindi appartiene a $\mathcal{B}$.

Per ogni insieme $B \in \mathcal{B}$ denotiamo con $M(B)$ l'insieme non vuoto dei maggioranti di B e notiamo che $M(B) \nsubseteq B$. Infatti ogni $b_0 \in M(B) \cap B$ è un elemento massimo di B. Poiché X non ha elementi massimali, esiste $x \in X$ con $x > b_0$, altrimenti b_0 sarebbe massimale. Ora $x \in M(B) \setminus B$. Abbiamo così dimostrato che $M(B) \setminus B \neq \emptyset$ per ogni $B \in \mathcal{B}$. Sia f una funzione di scelta definita per la famiglia $\{M(B) \setminus B : B \in \mathcal{B}\}$. Definiamo ora $g : \mathcal{B} \to X$ con $g(B) = f(M(B) \setminus B)$. Si noti che $X = M(\emptyset)$ e si ponga $x_0 = g(\emptyset) = f(X)$, allora il segmento iniziale $I_{\{x_0\}}(x_0)$ nell'insieme ben ordinato $(\{x_0\}, \leq)$ è vuoto e quindi $x_0 = g(I_{\{x_0\}}(x_0))$. Sia $\mathcal{A}$ la famiglia di tutti i sottoinsiemi $A \subseteq X$ tali che $(A, \leq)$ è ben ordinato e per ogni $a \in A$ si ha $a = g(I_A(a))$. Allora $I_A(a) \in \mathcal{B}$, $\{x_0\} \in \mathcal{A}$ che quindi non è vuoto.

Passo 1. Dimostriamo che se $A, B \in \mathcal{A}$, allora $A \subseteq B$ oppure $B \subseteq A$. Poniamo $C = \{c \in A \cap B : I_A(c) = I_B(c)\}$ e dimostriamo che C coincide con A o B. Supponiamo per assurdo $C \neq A$ e $C \neq B$, allora gli insiemi $A \setminus C$ e $B \setminus C$ non sono vuoti. Sia a il minimo elemento di $A \setminus C$ e sia b il minimo elemento di $B \setminus C$; esistono entrambi poiché A e B sono ben ordinati. Vogliamo dimostrare che $I_A(a) = I_B(b)$. Sia $x \in I_A(a)$. Allora $x \in A$ e $x < a$ implica $x \in C$. Quindi $x \in B$ e $I_A(x) = I_B(x)$. Notiamo che $x \neq b$ poiché $b \notin C$. Per l'esercizio 1.40, gli elementi $x, b \in B$ sono confrontabili. Supponiamo $x > b$. Allora da $I_A(x) = I_B(x)$ si avrebbe $b \in A$ e $b < x < a$. Di conseguenza $b \in C$, assurdo. Quindi $x < b$, cioè $x \in I_B(b)$. Analogamente si dimostra che

$$I_B(b) \subseteq I_A(a).$$

Ora l'uguaglianza $I_A(a) = I_B(b)$ implica $a = g(I_A(a)) = g(I_B(b)) = b$. Quindi $c = a = b \in A \cap B$ e $I_A(c) = I_B(c)$. Pertanto $c \in C$, assurdo. Questo dimostra che C coincide con A o B e di conseguenza abbiamo dimostrato che $A \subseteq B$ oppure $B \subseteq A$.

Passo 2. Sia $Y = \bigcup_{A \in \mathcal{A}} A$. Allora Y è una catena in X, in quanto per ogni coppia $a, b \in Y$, esistono $A \in \mathcal{A}$ e $B \in \mathcal{A}$ con $a \in A$ e $b \in B$. Per il passo 1, $A \subseteq B$ oppure $B \subseteq A$. Pertanto si avrà $a, b \in A$ oppure $a, b \in B$. Quindi vale $a \leq b$ oppure $b \leq a$, poiché A è totalmente ordinato per l'esercizio 1.40. Essendo Y una

catena, si ha $Y \in \mathcal{B}$. Poniamo $z = g(Y)$ e notiamo che $Z = Y \cup \{z\}$ risulta essere ben ordinato con l'ordine $\leq$ e $g(I_Z(z)) = g(Y) = z$. Quindi $Z \in \mathcal{A}$ e, poiché Z contiene propriamente Y, questo contraddice la definizione di Y. □

1.12 Prodotti cartesiani

Cominciamo con le potenze cartesiane, cioè prodotti cartesiani di un insieme per se stesso. Siano A ed I due insiemi non vuoti. L'insieme di tutte le applicazioni $f : I \to A$ si denota con A^I. Discuteremo ora la possibilità di vedere l'insieme A^I come un prodotto cartesiano. Cominciamo con le potenze cartesiane finite.

Lemma 1.66. *Sia A un insieme non vuoto. Esiste una biezione tra $A^{\{1,2\}}$ ed il prodotto cartesiano $A \times A$.*

DIMOSTRAZIONE. All'applicazione $f : \{1,2\} \to A$ mettiamo in corrispondenza la coppia ordinata $(f(1), f(2))$ di $A \times A$. Questo definisce un'applicazione $\varphi : A^{\{1,2\}} \to A \times A$. Inoltre φ è invertibile, avendo come inversa l'applicazione $\psi : A \times A \to A^{\{1,2\}}$ che alla coppia $(a,b) \in A \times A$ associa l'applicazione $f : \{1,2\} \to A$ definita da $f(1) = a$ e $f(2) = b$. □

La biezione φ del lemma 1.66 permette di identificare $A^{\{1,2\}}$ con il prodotto cartesiano $A \times A$ e scrivere più brevemente A^2. In questo modo non si distingue più tra una coppia ordinata di elementi di A ed un'applicazione $f : \{1,2\} \to A$. Analogamente possiamo definire il prodotto cartesiano

$$\underbrace{A \times A \times \ldots \times A}_{n \text{ volte}}$$

per ogni $n > 1$ come l'insieme di tutte le n-uple ordinate $(a_1, a_2, \ldots, a_n)$ di elementi di A, dove la n-upla $(a_1, a_2, \ldots, a_n)$ può essere vista come l'immagine dell'applicazione

$$f : \{1, 2, \ldots, n\} \to A \quad \text{definita da} \quad f(1) = a_1, \; f(2) = a_2, \; \ldots, \; f(n) = a_n.$$

In questo modo il prodotto cartesiano

$$\underbrace{A \times A \times \ldots \times A}_{n \text{ volte}},$$

che scriviamo più brevemente A^n, è proprio l'insieme $A^{\{1,2,\ldots,n\}}$.

Analogamente, possiamo considerare un'applicazione $f : \mathbb{N} \to A$, cioè un elemento di $A^{\mathbb{N}}$, come una successione infinita $a_1, a_2, \ldots, a_n, \ldots$ di elementi di A: è l'analogo della n-upla ordinata nel caso finito. L'insieme di tutte queste successioni è la potenza cartesiana infinita

$$\underbrace{A \times A \times \ldots \times A \times \ldots}_{\text{infinite volte}}.$$

Diamo una definizione nel caso generale.

Definizione 1.67. Dati due insiemi non vuoti A ed I, la *potenza cartesiana* A^I è l'insieme di tutte le applicazioni $f : I \to A$.

Nel caso di prodotti cartesiani di insiemi non necessariamente uguali bisogna ragionare diversamente anche se rimane una certa analogia.

Lemma 1.68. *Siano A e B due insiemi non vuoti. Allora esiste una biezione tra il prodotto cartesiano $A \times B$ e l'insieme X delle applicazioni $f : \{1, 2\} \to A \cup B$ con la proprietà $f(1) \in A$ e $f(2) \in B$.*

DIMOSTRAZIONE. All'applicazione $f \in X$ facciamo corrispondere la coppia ordinata $(f(1), f(2)) \in A \times B$. Questo definisce un'applicazione $\varphi : X \to A \times B$. Essa è invertibile, avendo come inversa l'applicazione $\psi : A \times B \to X$ che alla coppia $(a, b) \in A \times B$ associa l'applicazione $f : \{1, 2\} \to A \cup B$ definita da $f(1) = a$ e $f(2) = b$. □

Grazie alla biezione φ, identifichiamo il prodotto cartesiano $A \times B$ con l'insieme delle applicazioni $f : \{1, 2\} \to A \cup B$ con la proprietà $f(1) \in A$ e $f(2) \in B$. Lo scopo di introdurre un tale punto di vista diventa chiaro quando si passa a prodotti cartesiani di più di due insiemi.

Sia $n > 1$ e siano $A_1, A_2, \ldots, A_n$ degli insiemi non vuoti. Per $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$ definiamo un *n-upla ordinata* $(a_1, a_2, \ldots, a_n)$ come un'applicazione

$$f : \{1, 2, \ldots, n\} \to A_1 \cup A_2 \cup \ldots \cup A_n$$

con la proprietà

$$f(1) = a_1 \in A_1, \quad f(2) = a_2 \in A_2, \quad \ldots, \quad f(n) = a_n \in A_n,$$

che chiameremo funzione di scelta per la famiglia $A_1, \ldots, A_n$, seguendo la definizione 1.62.

Definizione 1.69. Il *prodotto cartesiano* $A_1 \times A_2 \times \ldots \times A_n$ è l'insieme di tutte le n-uple ordinate $(a_1, a_2, \ldots, a_n)$ con $a_1 \in A_1$, $a_2 \in A_2$, ..., $a_n \in A_n$.

Se tutti gli insiemi $A_1, A_2, \ldots, A_n$ coincidono con un dato insieme A, il prodotto cartesiano coincide con l'insieme A^n già visto.

In particolare, il prodotto cartesiano $\prod_{i \in I} A_i$ è non vuoto se I è finito, si veda l'esercizio 1.57.

Sia $n > 1$ e siano $A_1, A_2, \ldots, A_n$ insiemi non vuoti. Per $i = 1, 2, \ldots, n$ definiamo la *proiezione*

$$p_i : A_1 \times A_2 \times \ldots \times A_n \to A_i \quad \text{con} \quad p_i(a_1, a_2, \ldots, a_n) = a_i.$$

Queste applicazioni sono molto importanti per la definizione del prodotto cartesiano, si veda l'esercizio 1.56.

Per definire la potenza di un insieme A^I nella definizione 1.67, non abbiamo avuto bisogno dell'assioma della scelta. Se però vogliamo definire il prodotto cartesiano $\{A_i\}_{i \in I}$ per una famiglia I non vuota di insiemi non vuoti A_i, dobbiamo supporre che esista una funzione di scelta. Nel caso di prodotto cartesiano di famiglie arbitrarie utilizziamo la stessa definizione del prodotto cartesiano finito.

Definizione 1.70. Il *prodotto cartesiano* della famiglia $\{A_i\}_{i \in I}$ è l'insieme di tutte le funzioni di scelta della famiglia $\{A_i\}_{i \in I}$, denotato con $\prod_{i \in I} A_i$.

Si vede ora l'impatto dell'assioma della scelta sui prodotti cartesiani infiniti di insiemi. L'affermazione che il prodotto cartesiano $\prod_{i \in I} A_i$ sia non vuoto per ogni famiglia non vuota $\{A_i\}_{i \in I}$ di insiemi non vuoti è equivalente all'assioma della scelta. Nel caso di I finito non c'è bisogno di alcun ricorso all'assioma della scelta.

Analogamente a quanto fatto nel caso di prodotti finiti di insiemi, si può definire la proiezione anche nel caso infinito. Per $i \in I$ definiamo la *proiezione*

$$p_i : \prod_{i \in I} A_i \to A_i \quad \text{con} \quad p_i(f) = f(i)$$

per ogni funzione di scelta $f \in \prod_{i \in I} A_i$.

1.13 Numeri cardinali

In analogia con il caso della cardinalità $|A|$ di un insieme finito A, introduciamo qui un concetto di "misura" $|A|$ anche per insiemi infiniti A. Per evitare le difficoltà tecniche di definire rigorosamente il concetto di *numero cardinale* $|A|$, ci limiteremo a dire come si confrontano i numeri cardinali $|A|$ e $|B|$ di due insiemi. Diremo che A e B sono *equipotenti*, e scriveremo $|A| = |B|$, se esiste una biezione $A \to B$. Poiché è naturale avere $|A| \leq |B|$ per un sottoinsieme A di B, poniamo in generale $|A| \leq |B|$ se esiste un'applicazione iniettiva $A \to B$. Ricordiamo che, per il corollario 1.64, esiste un'applicazione iniettiva $A \to B$ se e solo se esiste un'applicazione suriettiva $B \to A$. Quindi $|A| \leq |B|$ se e solo se esiste un'applicazione suriettiva $B \to A$, si veda anche l'esercizio 1.60.

Scriveremo $|A| < |B|$ se vale $|A| \leq |B|$ ma non vale $|B| \leq |A|$. Nel seguente teorema di Cantor-Bernstein vediamo che $|A| = |B|$ equivale alla validità simultanea di $|A| \leq |B|$ e $|B| \leq |A|$. Questo teorema fornisce anche un metodo utile per la determinazione di insiemi equipotenti.

Teorema 1.71. (Teorema di Cantor-Bernstein) *Siano S e T due insiemi non vuoti. Se esistono iniezioni $S \to T$ e $T \to S$, allora esiste anche una biezione $S \to T$.*

DIMOSTRAZIONE. Consideriamo il seguente caso particolare del teorema, nel quale uno degli insiemi è sottoinsieme dell'altro e la rispettiva iniezione è l'inclusione. *Se $f : X \to X$ è un'applicazione iniettiva, allora per ogni suo sottoinsieme Y di X, tale che $f(X) \subseteq Y \subseteq X$, esiste una biezione $h : Y \to X$.* Vediamo subito che il caso generale si deduce facilmente da questo caso. Infatti per le iniezioni $r : S \to T$ e $q : T \to S$ è sufficiente considerare $X = S, Y = q(T)$ e $f = q \circ r$.

Per definire una biezione $g : Y \to X$ basta definire una biezione $s : Y \to f(X)$ e comporla con l'inversa di f su $f(X)$. Si consideri in Y la relazione R così definita:

$$xRy \iff \text{esistono } n, m \in \mathbb{N} \text{ con } f^n(x) = f^m(y).$$

Si dimostra facilmente che R è una relazione di equivalenza. Siano $\{C_i\}_{i\in I}$ le classi di equivalenza. Allora esse formano una partizione $\bigcup_{i\in I} C_i$ di Y. Ora definiamo s nel modo seguente. Sia $y \in C_i$. Se $C_i \subseteq f(X)$ poniamo $s(y) = y$. Se $C_i \not\subseteq f(X)$, poniamo $s(y) = f(y)$. Per far vedere che s è biettiva basta vedere che $s(Y) = f(X)$ e che s è iniettiva. Supponiamo $s(y) = s(y')$ per $y, y' \in Y$. Allora yRy' dalla definizione di s. Quindi y e y' appartengono alla stessa classe di equivalenza C_i. L'applicazione s ristretta a C_i coincide con l'identità di C_i oppure con la restrizione di f, ma in entrambi casi è iniettiva, pertanto $y = y'$. Per provare che s è anche suriettiva notiamo innanzitutto che $f(Y) \subseteq s(Y) \subseteq f(X)$. Infatti se $y \in Y$ appartiene a C_i per qualche $i \in I$, allora $f(y) \in C_i$. Pertanto se $C_i \subseteq f(X)$, si ha $s(f(y)) = f(y)$, se invece $C_i \not\subseteq f(X)$, si ha $s(y) = f(y)$. In entrambi i casi si conclude $f(y) \in s(Y)$. L'inclusione $s(Y) \subseteq f(X)$ viene dalla definizione di s. Resta quindi da provare $f(x) \in s(Y)$ per $x \in X \setminus Y$. Sia C_i la classe di equivalenza di $f(x)$ e sia $y \in C_i$. Allora esistono $n, m \in \mathbb{N}$ tali che $f^n(f(x)) = f^m(y)$. Se fosse $m > n$, avremmo $x = f^{m-n-1}(y) \in Y$, contro l'ipotesi fatta su x. Pertanto $m \leq n$, cioè $y = f^{n-m}(f(x)) \in f(X)$ da cui segue che tutta la classe C_i è contenuta in $f(X)$. Allora dalla defnzione di s segue $f(x) = s(f(x)) \in s(Y)$. □

Quando si ha $|A| = |B|$, diremo che A e B *hanno la stessa cardinalità* (sono equipotenti) e ci riferiamo al simbolo $|A|$ come *cardinalità* (o numero cardinale) di A.

Teorema 1.72. (Teorema di Hartogs) *Siano S e T due insiemi non vuoti. Allora esiste un'iniezione $S \to T$ oppure un'iniezione $T \to S$.*

DIMOSTRAZIONE. La famiglia $\mathcal{F}$ di tutte le applicazione iniettive $j_A : A \to T$, con $A \subseteq S$, è ordinata nel modo seguente: si pone $j_A \leq j_B$ per un'applicazione $j_B : B \to T$ se $A \subseteq B$ e $j_B(a) = j_A(a)$ per ogni $a \in A$. Dimostriamo ora che l'ordine $\leq$ di $\mathcal{F}$ è induttivo. Infatti sia $C = \{j_{B_i} : i \in I\}$ una catena in $\mathcal{F}$. Poniamo $B = \bigcup_{i\in I} B_i$ e definiamo $j_B : B \to T$ con $j_B(b) = j_{B_i}(b)$, se $b \in B_i$. La definizione è corretta, poiché se $b \in B_k$ per un altro $k \in I$, allora si ha $j_{B_i} \leq j_{B_k}$ oppure $j_{B_k} \leq j_{B_i}$. In entrambi casi $j_{B_k}(b) = j_{B_i}(b)$. Così abbiamo definito un elemento $j_B \in \mathcal{F}$ tale che $j_{B_i} \leq j_B$ for ogni $i \in I$. Quindi j_B è un maggiorante per la catena C e pertanto $\mathcal{F}$ è induttivo. Allora $\mathcal{F}$ ha elementi massimali per il lemma di Zorn; sia $f = j_{B_0} : B_0 \to T$ un tale elemento massimale. Se $B_0 = S$ abbiamo costruito un'iniezione $S \to T$. Supponiamo per assurdo che $B_0 \neq S$, cioè esiste un elemento $x \in S \setminus B_0$. Dimostriamo che in tal caso $f(B_0) = T$. Infatti, se esistesse $y \in T \setminus f(B_0)$, si potrebbe estendere f a $B' = B_0 \cup \{x\}$ ponendo $j_{B'}(b) = b$ per tutti i $b \in B_0$ e $j_{B'}(x) = y$. Allora $j_{B'}$ sarebbe iniettiva e $j_{B_0} < j_{B'}$, contraddicendo la massimalità di j_{B_0}. Pertanto $f(B_0) = T$ e per il teorema 1.63 esiste un'iniezione $T \to S$. □

Il teorema di Hartogs garantisce che per due insiemi S e T si ha $|S| \leq |T|$ oppure $|T| \leq |S|$. In altre parole, i numeri cardinali sono sempre paragonabili. Il teorema di Cantor-Bernstein garantisce inoltre che, se abbiamo simultaneamente $|S| \leq |T|$ e $|T| \leq |S|$, allora $|S| = |T|$.

Per il teorema di Cantor 1.18 vale $|X| < |\mathcal{P}(X)|$, si veda anche l'esercizio 1.62. Questo permette di trovare degli insiemi di cardinalità sempre più grandi.

Definizione 1.73. Un insieme X si dice *numerabile* se $|X| = |\mathbb{N}|$. Il primo numero cardinale infinito $|\mathbb{N}|$ si denota con $\aleph_0$ (si legge alef con zero).

Lemma 1.74. *$\mathbb{N} \times \mathbb{N}$ è numerabile.*

DIMOSTRAZIONE. Definiamo l'applicazione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, con

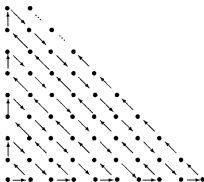
$$f(m,n) = 2^m(2n+1) - 1.$$

Allora f è iniettiva: supponiamo $f(m,n) = f(r,s)$. Se $f(m,n)$ è pari, allora $m = 0 = r$ e $n = f(m,n)/2 = f(r,s)/2 = s$. Se $f(m,n)$ è dispari, allora m ed n vengono univocamente determinati da $f(m,n)+1$. Inoltre f è suriettiva perché se $a \in \mathbb{N}$ è pari, allora $a = f(0, a/2)$, analogamente se a è dispari, $a+1$ individua univocamente $m, n \in \mathbb{N}$, grazie all'esercizio 1.17. Si veda anche il teorema fondamentale dell'aritmetica 3.12. □

Diamo un'idea di una dimostrazione grafica alternativa, che si ricorda facilmente. Definiamo un'applicazione biettiva $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ nel modo seguente:

$$h(0) = (0,0), \quad h(1) = (1,0), \quad h(2) = (0,1),$$

$$h(3) = (0,2), \quad h(4) = (1,1), \quad h(5) = (2,0), \quad \ldots$$

seguendo le frecce nel seguente diagramma

Nel seguito diremo che l'unione $\bigcup_{i \in I} A_i$ è numerabile se l'insieme degli indici I è numerabile. Chiaramente, dopo aver fissato una biezione $f : \mathbb{N} \to I$, possiamo scrivere tale unione anche come $\bigcup_{n=1}^{\infty} A_n$, dove $A_n = A_{f(n)}$.

Esempio 1.75. (a) Si può dimostrare che unioni finite o numerabili di insiemi numerabili sono insiemi numerabili (si veda l'esercizio 1.64 (b)).

(b) Sia X un insieme con $|X| > \aleph_0$. Allora per ogni sottoinsieme numerabile Y di X si ha $|X \setminus Y| = |X|$. Infatti l'insieme $X \setminus Y$ non è numerabile, perché altrimenti $X = Y \cup (X \setminus Y)$ risulterebbe numerabile per il punto (a). Per il teorema 1.42 esiste una iniezione $f : \mathbb{N} \to X$, sia Z la sua immagine. Allora Z è numerabile e quindi per il punto (a) anche $Z \cup Y$ è numerabile. Quindi, abbiamo due partizioni

$$X = (X \setminus (Z \cup Y)) \cup (Z \cup Y) \text{ e } X \setminus Y = (X \setminus (Z \cup Y)) \cup Z,$$

tali che $Z \cup Y$ e Z sono equipotenti in quanto numerabili. Allora anche X e $X \setminus Y$ sono equipotenti (per la costruzione di una biezione tra X e $X \setminus Y$ si veda l'esercizio 1.33).

Esempio 1.76. Il 7 Dicembre 1873 Georg Cantor (nato nel 1845 a S. Pietroburgo, morto nel 1918 a Halle), fondatore della *teoria degli insiemi*, dimostrò che l'insieme dei numeri reali non è numerabile. La cardinalità dell'insieme $\mathbb{R}$ è nota come *cardinalità del continuo* e si denota con $\mathfrak{c}$. Essa coincide con la cardinalità dell'insieme $\mathcal{P}(\mathbb{N})$, si veda il teorema 1.77.

In generale, poniamo $2^{|X|} = |2^X| = |\mathcal{P}(X)|$. Per il teorema di Cantor 1.18, si ha sempre $2^{|X|} > |X|$.

Teorema 1.77. *La cardinalità del continuo coincide con* $|\mathcal{P}(\mathbb{N})|$.

DIMOSTRAZIONE. Secondo uno dei due modi principali di introdurre i numeri reali, ogni numero reale r corrisponde ad una partizione $\mathbb{Q} = R_1 \cup R_2$ con la proprietà $x < y$ per ogni $x \in R_1$ ed ogni $y \in R_2$ (la coppia (R_1, R_2) di insiemi di numeri razionali si dice *sezione di Dedekind*). Poiché la partizione è completamente determinata dall'insieme R_1, l'assegnazione $r \mapsto R_1$ definisce un'iniezione di $\mathbb{R}$ in $\mathcal{P}(\mathbb{Q})$. Essendo $\mathcal{P}(\mathbb{Q})$ equipotente a $\mathcal{P}(\mathbb{N})$ questo dimostra $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$. D'altra parte $\mathcal{P}(\mathbb{N})$ è equipotente all'insieme $2^{\mathbb{N}}$ delle applicazioni $\mathbb{N} \to \{0,1\}$ per l'esercizio 1.54, cioè l'insieme delle successioni (a_n) di 0 e 1. Mettendo in corrispondenza alla successione (a_n) il numero reale $\sum_{n=1}^{\infty} a_n 2^{-n}$ definiamo un'applicazione $f : 2^{\mathbb{N}} \to \mathbb{R}$. Sia C il sottoinsieme di $2^{\mathbb{N}}$ che consiste delle successioni (a_n) che sono definitivamente costanti, cioè esiste un indice n_0 tale che a_n è costante per tutti gli $n \geq n_0$. Non è difficile vedere che f risulta iniettiva se ristretta al complemento C' di C in $2^{\mathbb{N}}$, quindi $|C'| \leq |\mathbb{R}|$. Essendo C numerabile, mentre $|2^{\mathbb{N}}| > |\mathbb{N}| = |C|$, si ha $|C'| = |2^{\mathbb{N}}|$ per l'esempio 1.75 (b). Poiché $|C'| = |\mathcal{P}(\mathbb{N})|$, si ha $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$. Per concludere che $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ basta applicare il teorema di Cantor–Bernstein.
□

Nel seguito, per insiemi X, Y denoteremo con $\max\{|X|, |Y|\}$ la più grande delle cardinalità tra $|X|$ e $|Y|$.

Teorema 1.78. *Se almeno uno degli insiemi X, Y è infinito, si ha*

$$|X \cup Y| = \max\{|X|, |Y|\}.$$

DIMOSTRAZIONE. Per il teorema di Hartogs possiamo supporre che $|X| \geq |Y|$. Per l'esercizio 1.68, esiste una partizione $X = X_1 \cup X_2$, tale che $|X_1| = |X_2| = |X|$. Quindi esiste un'iniezione $X \cup Y \to X_1 \cup X_2 = X$ e possiamo concludere che $|X \cup Y| \leq |X|$. Poiché $|X \cup Y| \geq |X|$, il teorema di Cantor-Bernstein permette di concludere che $|X \cup Y| = |X| = \max\{|X|, |Y|\}$. □

Per quanto riguarda il prodotto cartesiano abbiamo il seguente teorema.

Teorema 1.79. *Se almeno uno degli insiemi X, Y è infinito, si ha*

$$|X \times Y| = \max\{|X|, |Y|\}.$$

Per la dimostrazione del teorema 1.79, abbiamo bisogno del seguente lemma che tratta un caso particolare del teorema.

Lemma 1.80. $|X \times X| = |X|$ *per ogni insieme infinito X.*

DIMOSTRAZIONE. Sia A_0 un sottoinsieme numerabile di X. Per il lemma 1.74, esiste una biezione $i_{A_0} : A_0 \times A_0 \to A_0$. Si consideri la famiglia $\mathcal{A}$ delle coppie (A, i_A), dove $A_0 \subseteq A \subseteq X$ e $i_A : A \times A \to A$ è una biezione che estende i_{A_0}. Si consideri in $\mathcal{A}$ la relazione $\leq$ definita da $(A, i_A) \leq (B, i_B)$ se e solo se $A \subseteq B$ e $i_B \restriction_{A \times A} = i_A$. Non è difficile provare che $\leq$ è un ordine per il quale $(\mathcal{A}, \leq)$ è un insieme ordinato induttivo. Per il lemma di Zorn esiste un elemento massimale $(M, i_M) \in \mathcal{A}$. Chiaramente $(M, i_M) \in \mathcal{A}$ implica

$$|M \times M| = |M|. \tag{9}$$

Se $|M| = |X|$, allora abbiamo anche $|X \times X| = |M \times M|$, per l'esercizio 1.58, e quindi l'uguaglianza (9) assieme all'ipotesi fatta implica $|X \times X| = |X|$. Supponiamo per assurdo che $|M| \neq |X|$. Poiché $|M| \leq |X|$, resta la sola possibilità $|M| < |X|$. D'altra parte $X = M \cup (X \setminus M)$, quindi $|X \setminus M| \geq |M|$ per il teorema 1.78. Possiamo trovare un sottoinsieme $N \subseteq X \setminus M$ con $|N| = |M|$. Ora $M' = M \cup N$ contiene M propriamente, e $M' \times M' = (M \times M) \cup D$, dove $D = (M \times N) \cup (N \times M) \cup (N \times N)$. Si ha

$$|N \times M| = |M \times N| = |N \times N| = |M| = |N|,$$

da cui, per il teorema 1.78, $|D| = |N|$. Allora esiste una biezione $D \to N$, che, assieme alla biezione $i_M : M \times M \to M$ porge una biezione $i_{M'} : M' \times M' \to M'$ che estende i_M. Quindi $(M', i_{M'}) \in \mathcal{A}$ e $(M, i_M) < (M', i_{M'})$, assurdo. Pertanto $|M| = |X|$. □

DIMOSTRAZIONE DEL TEOREMA 1.79. Per il teorema di Hartogs possiamo supporre $|X| \geq |Y|$. Per il lemma 1.80 si ha $|X \times X| = |X|$. Allora

$$|X| \geq |X \times X| \geq |X \times Y| \geq |X|. \qquad \square$$

Di conseguenza, se almeno uno degli insiemi X, Y è infinito la cardinalità del loro prodotto e della loro unione coincidono:

$$|X \times Y| = |X \cup Y| = \max\{|X|, |Y|\}.$$

Si può dimostrare per induzione che

$$|X_1 \times \ldots \times X_n| = |X_1 \cup \ldots \cup X_n| = \max\{|X_1|, \ldots, |X_n|\}$$

$$\text{e} \quad |X^n| = |X|$$

per ogni ogni numero naturale $n > 0$ se X e almeno uno degli insiemi $X_1, \ldots, X_n$ è infinito. Vari casi concreti si possono trovare nell'esercizio 1.64.

1.14 Esercizi su insiemi e relazioni

Esercizio 1.1 Si descriva l'insieme $\mathcal{P}(\{1,2,3\})$.

Esercizio 1.2 Siano A e B due insiemi. Si dimostri che

$$A \subseteq B \quad \text{se e solo se} \quad \mathcal{P}(A) \subseteq \mathcal{P}(B).$$

Esercizio 1.3 Dimostrare che l'intersezione $X \cap Y$ è il più grande insieme che soddisfa $Z \subseteq X$ e $Z \subseteq Y$. Più precisamente, se $Z \subseteq X$ e $Z \subseteq Y$, allora anche $Z \subseteq X \cap Y$.

Esercizio 1.4 Provare che, dati due insiemi S e T, risulta

(a) $\mathcal{P}(S \cap T) = \mathcal{P}(S) \cap \mathcal{P}(T)$
(b) $\mathcal{P}(S) \cup \mathcal{P}(T) \subseteq \mathcal{P}(S \cup T)$
(c) $\mathcal{P}(S) \cup \mathcal{P}(T) = \mathcal{P}(S \cup T)$ se e solo se $S \subseteq T$ oppure $T \subseteq S$.

Esercizio 1.5 Siano S, T e V insiemi. Provare che valgono le proprietà distributive della differenza rispetto all'intersezione e all'unione:

(a) $(S \cap T) \setminus V = (S \setminus V) \cap (T \setminus V)$;
(b) $(S \cup T) \setminus V = (S \setminus V) \cup (T \setminus V)$;
(c) mostrare con un esempio che non valgono per la differenza le proprietà associativa e commutativa.

Esercizio 1.6 Siano A e B due insiemi. Si dimostri che $\{A \setminus B, B \setminus A, A \cap B\}$ è una partizione di $A \cup B$.

Esercizio 1.7 Sia $f : \mathbb{R} \to \mathbb{R}$ l'applicazione definita da

$$f(x) = \begin{cases} x + \frac{x+1}{x-1}, & \text{se } x \neq 1 \\ 0, \quad \text{se} & x = 1. \end{cases}$$

Si determini se f è iniettiva e se f è suriettiva.

Esercizio 1.8 Si dica quali delle applicazioni definite negli esempi 1.12 e 1.13 sono iniettive, suriettive o biettive.

Esercizio 1.9 Sia $f : \mathbb{R} \to \mathbb{R}$ una delle seguenti funzioni. Si dica quale di queste funzioni è iniettiva, suriettiva o biettiva:

$$f(x) = 2^x; \qquad f(x) = 3x^2 - \sqrt{5}; \qquad f(x) = \mathrm{sen}(x);$$

$$f(x) = \begin{cases} x, & \text{se } x < 0 \\ x^2, & \text{se } x \geq 0 \end{cases}$$

Esercizio 1.10 Sia $f : X \longrightarrow Y$ una funzione e $B \subseteq Y$.

(a) Si provi che $f(f^{-1}(B)) \subseteq B$.
(b) Si costruisca un esempio per cui $f(f^{-1}(B)) \neq B$.
(c) Quando vale $f(f^{-1}(B)) = B$?

Esercizio 1.11 Siano A un insieme e B un sottoinsieme di A, $\emptyset \neq B \neq A$. Sia

$$f : \mathcal{P}(A) \longrightarrow \mathcal{P}(A) \quad \text{la funzione definita da } f(X) = B \setminus X.$$

(a) Si provi che f non è né iniettiva né suriettiva;
(b) si descriva $f^{-1}(\{B\})$.

Esercizio 1.12 Siano A un insieme e B un sottoinsieme di A, $\emptyset \neq B \neq A$.

$$f : \mathcal{P}(A) \longrightarrow \mathcal{P}(A) \quad \text{la funzione definita da } f(X) = B \cap X.$$

(a) Si dica se f è iniettiva;
(b) si trovi l'immagine di f;
(c) si descriva $f^{-1}(\{B, A, \emptyset\})$.

Esercizio 1.13 Sia f una funzione da un insieme A in sé. Si supponga che $f \circ f \circ f = id_A$. Si può concludere che f è biettiva?

Esercizio 1.14 Sia X un'insieme e sia $j_X : X \to \mathcal{P}(X)$ l'applicazione definita da $j_X(x) = \{x\}$. Sia $f : X \to Y$ un'applicazione e sia $f_* : \mathcal{P}(X) \longrightarrow \mathcal{P}(Y)$ la funzione così definita $f_*(B) = f(B)$. Si provi che:

(a) j_X è iniettiva e che $f_* \circ j_X = j_Y \circ f$;
(b) f è iniettiva se e solo se f_* è iniettiva,
(c) f è suriettiva se e solo se f_* è suriettiva.

Esercizio 1.15 Sia $f : X \to Y$ un'applicazione e sia $f^* : \mathcal{P}(Y) \to \mathcal{P}(X)$ la funzione così definita $f^*(B) = f^{-1}(B) = \{a \in X : f(a) \in B\}$. Si provi che:

(a) f^* è iniettiva se e solo se f è suriettiva,
(b) f^* è suriettiva se e solo se f è iniettiva.

Esercizio 1.16 * Siano (N_1, s_1) e (N_2, s_2) due insiemi che soddisfano gli assiomi di Peano, allora esiste un'unica biezione $f : N_1 \to N_2$, tale che se $\{a_1\} = N_1 \setminus s_1(N_1)$ e $\{a_2\} = N_2 \setminus s_2(N_2)$, si ha $f(a_1) = a_2$ e $f(s_1(n)) = s_2(f(n))$ per ogni $n \in N_1$.

Esercizio 1.17 Dimostrare che per ogni numero naturale $k > 0$ esiste un'unica coppia (m, n) di numeri naturali tali che $k = 2^m(2n + 1)$.

Esercizio 1.18 Usando il principio di induzione, provare che per ogni numero naturale $n \geq 1$ risulta:

(a) $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.
(b) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.
(c) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.
(d) $1^4 + 2^4 + 3^4 + \ldots + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$.
(e) $1^5 + 2^5 + 3^5 + \ldots + n^5 = \frac{n^2(n+1)^2(2n^2+2n-1)}{12}$.
(f) $1^6 + 2^6 + 3^6 + \ldots + n^6 = \frac{n(n+1)(2n+1)(3n^4+6n^3-3n+1)}{42}$.
(g) $1^7 + 2^7 + 3^7 + \ldots + n^7 = \frac{n^2(n+1)^2(3n^4+6n^3-n^2-4n+2)}{24}$.

Esercizio 1.19 Usando il principio di induzione, provare che per ogni numero naturale n risulta:

$$\frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \ldots + \frac{1}{2^n} = 2 - \frac{1}{2^n}.$$

Esercizio 1.20 Scrivere nella forma abbreviata tutte le somme degli esercizi 1.18 e 1.19.

Esercizio 1.21 Provare che per ogni numero naturale $n \geq 1$, si ha:

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} \geq \sqrt{n}.$$

Esercizio 1.22 Usando il principio di induzione, provare che per ogni numero naturale $n \geq 1$, si ha:

(a)

$$\sum_{k=1}^{n} kq^{k-1} = \frac{nq^{n+1} - (n+1)q^n + 1}{(1-q)^2},$$

dove q è un numero reale fisso diverso da 1;

(b)

$$\sum_{k=2}^{n} \frac{1}{k^2 - 1} = \frac{3}{4} - \frac{2n+1}{2n(n+1)} \text{ per } n \geq 2;$$

(c)

$$\sum_{k=1}^{n} \frac{1}{n+k} \geq \frac{7}{12} \text{ per } n \geq 2.$$

Esercizio 1.23 Siano n e $a_1 < a_2 < \ldots < a_n$ numeri naturali, $n \geq 1$. Provare che

$$\left(\sum_{k=1}^{n} a_k\right)^2 \leq \sum_{k=1}^{n} a_k^3.$$

Esercizio 1.24 Sia dato un intero $n > 1$. Dimostrare che il massimo dei valori di $\binom{n}{k}$ per $k \in \{0, \ldots, n\}$ è assunto per $k = \frac{n}{2}$ se n è pari e per $k = \frac{n+1}{2}$ e per $k = \frac{n-1}{2}$ se n è dispari.

Esercizio 1.25 Trovare l'errore nello svolgimento dell'esempio 1.61.

Esercizio 1.26 * Dimostrare che la media aritmetica è maggiore o uguale alla media geometrica; cioè, dati $a_i \in \mathbb{R}$, con $a_i > 0$, per $i = 1, 2, \ldots, n$ si dimostri che

$$\sqrt[n]{a_1 \cdot a_2 \cdot \ldots \cdot a_n} \leq \frac{a_1 + a_2 + \ldots + a_n}{n}.$$

Esercizio 1.27 Dimostrare che la media geometrica è maggiore o uguale alla media armonica; cioè, dati $a_i \in \mathbb{R}$, con $a_i > 0$, per $i = 1, 2, \ldots, n$ si dimostri che

$$\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 \cdot a_2 \cdot \ldots \cdot a_n}.$$

Esercizio 1.28 Siano A e B due insiemi finiti. Si dimostri che $A \cap B$ è finito e $|A \cup B| = |A| + |B| - |A \cap B|$ e quindi anche $A \cup B$ è finito.

Esercizio 1.29 * Siano A, B e C tre insiemi finiti. Si dimostri che

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|.$$

Trovare una formula per la cardinalità dell'unione di n insiemi finiti $\bigcup_{k=1}^{n} A_k$, dove $n > 3$.

Esercizio 1.30 * Sia $f : X \to X$ un'applicazione iniettiva, ma non suriettiva. Si provi che per ogni $x \in X \setminus f(X)$ esiste un'applicazione iniettiva $h : \mathbb{N} \to X$ con $h(0) = x$.

Esercizio 1.31 Se un insieme X ammette una suriezione $X \to X$ che non è iniettiva, dimostrare che X è infinito nel senso di Cantor.

Esercizio 1.32 Sia X un insieme non vuoto e sia $\mathcal{A} = \{A_i : i \in I\}$ una famiglia di sottoinsiemi di X tali che

(a) $X = \bigcup_{i \in I} A_i$,
(b) $\mathcal{A}$ è chiusa per intersezioni, cioè intersezioni di elementi di $\mathcal{A}$ stanno in $\mathcal{A}$.

Dimostrare che la relazione $\sim$ su X definita da $x \sim y$ se e solo se per ogni $i \in I$ si ha $x \in A_i$ se e solo se $y \in A_i$, è una relazione di equivalenza.

Esercizio 1.33 Sia $X = \bigcup_{i \in I} C_i$ una partizione e sia Y un sottoinsieme di X. Se per ogni $i \in I$ $h_i : C_i \to C_i \cap Y$ è un'applicazione iniettiva, si provi che l'applicazione $h : X \to Y$ definita da $h(x) := h_i(x)$ per $x \in C_i$ è iniettiva. Inoltre h è biettiva se e solo se ogni h_i è biettiva. In particolare, se per ogni $i \in I$ esiste una biezione $h_i : C_i \to C_i \cap Y$, provare che esiste anche una biezione $h : X \to Y$.

Esercizio 1.34 Sia X un insieme infinito. Dimostrare che:

(a) per ogni elemento $x \in X$, esiste una biezione fra X e $X \setminus \{x\}$;
(b) per ogni insieme finito $F \subseteq X$, esiste una biezione fra X e $X \setminus F$.

Esercizio 1.35 Dimostrare che ogni insieme parzialmente ordinato e finito è induttivo.

Esercizio 1.36 Dimostrare che ogni reticolo finito è limitato.

Esercizio 1.37 Sia A un insieme non vuoto finito o numerabile. Dimostrare che A ammette una relazione di buon ordine.

Esercizio 1.38 Sia X un insieme non vuoto; allora l'insieme parzialmente ordinato $(\mathcal{P}(X), \subseteq)$ è un reticolo limitato.

Esercizio 1.39 Si dia un esempio di un reticolo che ha un sottoinsieme ordinato che non è un reticolo.

Esercizio 1.40 Dimostrare che ogni ordine buono è anche totale.

Esercizio 1.41 Calcolare il numero delle relazioni di equivalenza su un insieme di 2, 3, 4 o 5 elementi.

Esercizio 1.42 Dimostrare che ogni insieme non vuoto parzialmente ordinato e finito ammette elementi massimali ed elementi minimali.

Esercizio 1.43 Sia $\leq$ un ordine su un insieme X e Y un sottoinsieme non vuoto di X. Si provi che:

(a) se Y ha un minimo (massimo), esso è unico;
(b) se Y ha un estremo superiore (inferiore) in X, esso è unico.

Esercizio 1.44 Si provi che se A è totalmente ordinato e $a \in A$, allora a è il massimo di A se e solo se a è un elemento massimale di A.

Esercizio 1.45 Sia $\mathbb{N}$ l'insieme dei numeri naturali. Si dimostri che $\mathbb{N}$ con la relazione di divisibilità definita da $n|m$ se e solo se esiste $r \in \mathbb{N}$ tale che $m = rn$, è un insieme parzialmente ordinato che ammette massimo e minimo.

Esercizio 1.46 Individuare tutte le catene di lunghezza 4 nell'insieme ordinato per divisibilità di tutti i divisori di 20. Dimostrare che le catene di lunghezza 2 sono 12.

Esercizio 1.47 Sia $(X, \leq)$ un reticolo e a un suo elemento massimale, allora a è massimo.

Esercizio 1.48 Siano A, B e C gli insiemi dei divisori propri di 30, 56 e 120, rispettivamente, ordinati per divisibilità. Si determinino gli elementi massimali e minimali di A, B e C.

Esercizio 1.49 Siano $(A, \leq)$ e $(B, \leq')$ due insiemi parzialmente ordinati. Allora sul prodotto cartesiano $A \times B$ consideriamo le relazioni binarie $\prec$ e $\lhd$ definite come segue

$$(a, b) \prec (a_1, b_1) \text{ se } a < a_1 \text{ oppure } a = a_1 \text{ e } b \leq' b_1,$$
$$(a, b) \lhd (a_1, b_1) \text{ se } a \leq a_1 \text{ e } b \leq' b_1.$$

Dimostrare che

(a) $\prec$ e $\lhd$ sono ordini parziali chiamati, rispettivamente *ordine lessicografico* e *prodotto cartesiano* di $\leq$ e $\leq'$;
(b) $\prec$ è totale se $\leq$ e $\leq'$ sono totali, mentre $\lhd$ non è totale se $|A| > 1$ e $|B| > 1$.

Esercizio 1.50 Siano $A = \{1, 2, \ldots, n\}$ e $B = \{1, 2, \ldots, m\}$ con l'ordine usuale e $X = A \times B$ munito dell'ordine $\lhd$, definito nell'esercizio 1.49. L'*altezza* di un insieme parzialmente ordinato finito L è il massimo tra le lunghezze delle catene di L e sarà denotata con $h(L)$. Dimostrare che $h(X) = m + n - 1$.

Esercizio 1.51 Siano A e B insiemi parzialmente ordinati finiti e $X = A \times B$ munito dell'ordine $\lhd$, definito nell'esercizio 1.49. Dimostrare che

$$h(X) = h(A) + h(B) - 1,$$

ove $h(X)$ è l'altezza definita nell'esercizio 1.50.

Esercizio 1.52 Sia $(L, \leq)$ un reticolo, allora sull'insieme L^X definiamo un ordine parziale nel modo seguente:

$$f, g \in L^X \quad f \prec g \iff f(x) \leq g(x) \text{ per ogni } x \in X.$$

Si dimostri che $(L^X, \prec)$ è un reticolo.

Esercizio 1.53 Sia $(S, \leq)$ un insieme ordinato e nell'insieme S^S delle applicazioni di S in sé si consideri la relazione binaria $\mathcal{R}$, definita ponendo $f \mathcal{R} g$ se e solo se $f(x) \leq g(x)$ per ogni $x \in S$. Provare che $\mathcal{R}$ è una relazione d'ordine e che $\mathcal{R}$ risulta totale se e solo se S è costituito da un solo elemento.

Esercizio 1.54 Siano X insieme non vuoto e $A \in \mathcal{P}(X)$. Si definisca la funzione caratteristica $\chi_A : X \to \{0, 1\}$

$$\chi_A(x) = \begin{cases} 1 \text{ se } x \in A, \\ 0 \text{ se } x \in X, x \notin A. \end{cases}$$

Dimostrare che l'applicazione $\varphi : \mathcal{P}(X) \to 2^X$ definita da $\varphi(A) = \chi_A$ è una biezione.

Esercizio 1.55 Dimostrare che $|\mathcal{P}(X)| = 2^{|X|}$ per ogni insieme finito X.

Esercizio 1.56 Sia $n > 1$ e siano $A_1, A_2, \ldots, A_n$ insiemi non vuoti.

(a) Dimostrare che la proiezione $p_i : A_1 \times A_2 \times \ldots \times A_n \to A_i$ definita da

$$p_i(a_1, a_2, \ldots, a_n) = a_i,$$

per $i = 1, .., n$ è suriettiva, ma non necessariamente iniettiva.

(b) Siano $B_1, B_2, \ldots, B_n$ insiemi non vuoti e siano $f_i : A_i \to B_i$ applicazioni $(i = 1, 2, \ldots, n)$. Si definisca l'applicazione

$$f_1 \times f_2 \times \ldots \times f_n : A_1 \times A_2 \times \ldots \times A_n \to B_1 \times B_2 \times \ldots \times B_n$$

con $(f_1 \times f_2 \times \ldots \times f_n)(a_1, a_2, \ldots, a_n) = (f_1(a_1), f_2(a_2), \ldots, f_n(a_n))$.
Dimostrare che:
- $p_i \circ (f_1 \times f_2 \times \ldots \times f_n) = f_i$ per $i = 1, 2, \ldots, n$;
- $f_1 \times f_2 \times \ldots \times f_n$ è iniettiva (rispettivamente suriettiva) se e solo se tutte le applicazioni f_i sono iniettive (rispettivamente suriettive).

Esercizio 1.57 Sia $n > 1$ e siano $A_1, A_2, \ldots, A_n$ insiemi non vuoti.

(a) Trovare una biezione tra i prodotti

$$(A_1 \times A_2 \times \ldots \times A_{n-1}) \times A_n \quad \text{e} \quad A_1 \times A_2 \times \ldots \times A_n.$$

(b) In caso di insiemi finiti dimostrare che $|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$.

Esercizio 1.58 Siano $\{A_i\}_{i \in I}$ e $\{B_j\}_{j \in J}$ due famiglie di insiemi non vuoti con $I \neq \emptyset \neq J$. Se esiste una biezione $\varphi : I \to J$ e per ogni $i \in I$ una biezione

$$\psi_i : A_i \to B_{\varphi(i)},$$

allora esiste anche una biezione

$$\prod_{i \in I} A_i \to \prod_{j \in J} B_j.$$

Esercizio 1.59 Sia $\{A_i\}_{i \in I}$ una famiglia di insiemi non vuoti e $\emptyset \neq J \subset I$. Dimostrare che esiste una biezione

$$\prod_{i \in I} A_i \to \prod_{j \in J} A_j \times \prod_{i \in I \setminus J} A_i.$$

Esercizio 1.60 Dimostrare che vale $|A| \leq |B|$ per due insiemi A, B se e solo se esiste un'applicazione suriettiva $B \to A$.

Esercizio 1.61 * Dimostrare che esiste una biezione fra l'intervallo chiuso $[0, 1]$ e l'insieme $\mathbb{R}$ dei numeri reali. Costruire esplicitamente una tale biezione.

Esercizio 1.62 Per ogni insieme X, si ha $|X| < |\mathcal{P}(X)|$.

Esercizio 1.63 Dimostrare che un insieme infinito X è numerabile se e solo se esiste un'applicazione suriettiva $\mathbb{N} \to X$.

Esercizio 1.64 Dimostrare che:

(a) i seguenti insiemi sono numerabili: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$;
(b) se $A_1, \ldots, A_n, \ldots$ sono insiemi numerabili, allora anche gli insiemi $\bigcup_{n=1}^{\infty} A_n$ e $A_1 \times \ldots \times A_k$ sono numerabili per ogni k.

Esercizio 1.65 Siano X ed Y due insiemi che ammettono delle partizioni

$$X = \bigcup \{X_i : i \in I\} \quad \text{e} \quad Y = \bigcup \{Y_i : i \in I\}$$

con $|X_i| = |Y_i|$ per ogni $i \in I$. Provare che X ed Y sono equipotenti.

Esercizio 1.66 Sia X un insieme infinito. Dimostrare che esiste una partizione $\{X_i : i \in I\}$ di X in insiemi numerabili.

Esercizio 1.67 Si dimostri che $|X| = |X \times \{0, 1\}|$ per ogni insieme infinito.

Esercizio 1.68 Se X è un insieme infinito, provare che esiste una partizione

$$X = X_1 \cup X_2 \quad \text{di} \quad X \quad \text{con} \quad |X_1| = |X_2| = |X|.$$

I numeri interi, razionali, reali e complessi

In questo capitolo si introducono i numeri razionali, reali e complessi. Nel primo paragrafo si costruiscono i numeri interi formalmente a partire dai numeri naturali. Gran parte di questo paragrafo può essere tralasciato da chi preferisce una visione più intuitiva e meno formale dei numeri interi.

Nel secondo paragrafo si danno alcuni cenni alle proprietà dei numeri razionali e reali, mentre la costruzione dei numeri razionali viene rimandata al successivo teorema 10.14 in una situazione più generale. Nel terzo paragrafo vengono introdotti i numeri complessi e le operazioni tra essi, mentre nel quarto ne viene data un'interpretazione geometrica.

2.1 I numeri interi

Dato l'insieme dei numeri naturali $\mathbb{N}$, si costruisce facilmente in modo abbastanza intuitivo l'insieme dei numeri interi come l'insieme delle differenze di numeri naturali.

Diamo qui, per completezza, una costruzione rigorosa dei numeri interi. Per far questo, partiamo dal prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ e definiamo una relazione tra le coppie di $\mathbb{N} \times \mathbb{N}$ nel modo seguente:

$$(a, b) \sim (c, d) \iff a + d = b + c.$$

Si vede immediatamente che la relazione $\sim$ è riflessiva e simmetrica. Verifichiamo la transitività: da $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$ segue $a + d = b + c$ e $c + f = d + e$. Aggiungendo f alla prima uguaglianza, si ha $a + d + f = b + c + f = b + d + e$, ad cui $a + f = b + e$ per il lemma 1.34(c), cioè $(a, b) \sim (e, f)$.

Denotiamo con $[(a, b)]$ la classe di equivalenza di (a, b) rispetto a questa relazione. Sia $\mathbb{Z}$ l'insieme quoziente $(\mathbb{N} \times \mathbb{N})/\sim$ delle classi di equivalenza. Allora $\mathbb{Z}$ è l'insieme dei *numeri interi*.

Definiamo una somma in $\mathbb{Z}$ nel modo seguente:

$$[(a, b)] + [(c, d)] = [(a + c, b + d)].$$

Allora + è ben definita e gode delle proprietà commutativa e associativa.

Lemma 2.1. *Sia '+' la somma definita in* $\mathbb{Z}$ *da*

$$[(a,b)] + [(c,d)] = [(a+c, b+d)].$$

Allora '+' è ben definita e per ogni $[(a,b)], [(c,d)], [(e,f)] \in \mathbb{Z}$ *valgono le seguenti proprietà:*

(1) $[(a,b)] + [(c,d)] = [(c,d)] + [(a,b)]$ *(commutatività);*
(2) $([(a,b)] + [(c,d)]) + [(e,f)] = [(a,b)] + ([(c,d)] + [(e,f)])$ *(associatività);*
(3) $[(a,b)] + [(0,0)] = [(a,b)]$ *(esistenza dello zero);*
(4) $[(a,b)] + [(b,a)] = [(0,0)]$ *(esistenza di un opposto).*

DIMOSTRAZIONE. Lasciamo per esercizio le verifiche della buona definizione e delle proprietà commutativa e associativa. Verifichiamo (3) e (4).

$$[(a,b)] + [(0,0)] = [(a+0, b+0)] = [(a,b)],$$

$$[(a,b)] + [(b,a)] = [(a+b, a+b)] = [(0,0)],$$

in quanto $a + b + 0 = a + b + 0$. □

Possiamo anche definire un prodotto in $\mathbb{Z}$ come segue

$$[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)].$$

Valgono le seguenti proprietà.

Lemma 2.2. *Sia · il prodotto definito in* $\mathbb{Z}$ *da* $[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)]$. *Allora · è ben definito e per ogni* $[(a,b)], [(c,d)], [(e,f)] \in \mathbb{Z}$ *valgono le seguenti proprietà:*

(1) $[(a,b)] \cdot [(c,d)] = [(c,d)] \cdot [(a,b)]$ *(commutatività);*
(2) $([(a,b)] \cdot [(c,d)]) \cdot [(e,f)] = [(a,b)] \cdot ([(c,d)] \cdot [(e,f)])$ *(associatività);*
(3) $[(a,b)] \cdot [(1,0)] = [(a,b)]$ *(esistenza di identità);*
(4) $[(a,b)] \cdot ([(c,d)] + [(e,f)]) = [(a,b)] \cdot (c,d)] + [(a,b)] \cdot [(e,f)]$ *(distributività rispetto alla somma).*

DIMOSTRAZIONE. Lasciamo per esercizio le verifiche della buona definizione e delle proprietà commutativa e associativa. Verifichiamo (3) e (4).

$$[(a,b)] \cdot [(1,0)] = [(a \cdot 1, b \cdot 1)] = [(a,b)].$$

$$[(a,b)] \cdot ([(c,d)] + [(e,f)]) = [(a,b)] \cdot [(c+e, d+f)] =$$
$$= [(ac+ae+bd+bf, ad+af+bc+be)] =$$
$$= [(ac+bd, ad+bc)] + [(ae+bf, af+be)] = [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)].$$

□

Definiamo un'altra relazione tra due numeri interi, $[(a,b)] \leq [(c,d)]$ se e solo se $a+d \leq b+c$ in $\mathbb{N}$. Tale relazione è riflessiva. Proviamo che è antisimmetrica: $[(a,b)] \leq [(c,d)]$ e $[(c,d)] \leq [(a,b)]$ danno $a+d \leq b+c$ e $c+b \leq a+d$, da cui segue l'uguaglianza $a+d = b+c$, cioè $[(a,b)] = [(c,d)]$. Analogamente si prova che $\leq$ è transitiva. Pertanto $\leq$ è una relazione d'ordine in $\mathbb{Z}$.

Costruiamo ora un'applicazione iniettiva da $\mathbb{N}$ in $\mathbb{Z}$ che "conserva" la somma e il prodotto, come illustriamo di seguito. Sia $j : \mathbb{N} \to \mathbb{Z}$ l'applicazione così definita $j(n) = [(n,0)]$. Allora $j(n) = j(m)$ implica che $[(n,0)] = [(m,0)]$, cioè $n = n+0 = m+0 = m$. Inoltre

$$j(n+m) = [(n+m,0)] = [(n,0)] + [(m,0)] = j(n) + j(m)$$

e

$$j(nm) = [(nm,0)] = [(n,0)] \cdot [(m,0)] = j(n) \cdot j(m).$$

Come nel caso dei naturali, anche nel prodotto tra due numeri interi, ometteremo spesso il simbolo $\cdot$.

Identifichiamo dunque $\mathbb{N}$ con $j(\mathbb{N})$. Poniamo $-n = [(0,n)]$, per ogni $n \in \mathbb{N}$ e definiamo la *differenza* tra due elementi come $n - m = n + (-m)$. Allora ogni elemento di $\mathbb{Z}$ si scrive come $[(n,m)] = [(n,0)] + [(0,m)] = n + (-m) = n - m$. Osserviamo che, se $n \geq m$, si ha $[(n,m)] = [(n-m,0)] = n - m \in \mathbb{N}$ e se $m \geq n$ si ha $[(n,m)] = [(0,m-n)] = -(m-n)$ con $m-n \in \mathbb{N}$. Pertanto tutti gli elementi di $\mathbb{Z}$ che non stanno in $\mathbb{N}$ si possono scrivere nella forma $-n$ per qualche $n \in \mathbb{N}$. Si osservi che la relazione d'ordine definita in $\mathbb{Z}$ estende la relazione d'ordine di $\mathbb{N}$: infatti, se $n, m \in \mathbb{N}$, si ha $[(n,0)] \leq [(m,0)]$ se e solo se $n \leq m$. Inoltre se $n \in \mathbb{N}$, si ha $n \geq 0$ e $-n \leq 0$.

Diremo che un numero intero z è *negativo* se $z < 0$ e diremo che è *positivo* se $z > 0$.

Osserviamo che, se $n, m \in \mathbb{N}$, si ha $n(-m) = -(nm)$, infatti

$$[(n,0)] \cdot [(0,m)] = [(0,nm)].$$

Da (d) del lemma 1.35, segue allora

Lemma 2.3. *Per ogni $z_1, z_2 \in \mathbb{Z}$ si ha $z_1 z_2 = 0$ se e solo se $z_1 = 0$ oppure $z_2 = 0$.*

2.2 I numeri razionali e reali

Dall'insieme $\mathbb{Z}$ con le operazioni $+$ e $\cdot$ costruito nel paragrafo 2.1, seguendo lo stesso schema, si può costruire l'insieme $\mathbb{Q}$ dei *numeri razionali* contenente $\mathbb{Z}$ e fornito di due operazioni $+$ e $\cdot$ che estendono quelle di $\mathbb{Z}$ e godono delle stesse proprietà descritte nei lemmi 2.1, 2.2 e 2.3. Inoltre per ogni elemento $b \in \mathbb{Z}$, $b \neq 0$ esiste in $\mathbb{Q}$ un unico elemento denotato con $\frac{1}{b}$ tale che $b\frac{1}{b} = 1$. Per $a \in \mathbb{Z}$ il prodotto $a\frac{1}{b}$ si denota con $\frac{a}{b}$ ed ogni elemento di $\mathbb{Q}$ si può scrivere in questa forma. Evitiamo di dare esplicitamente tale costruzione perché verrà fatta in una situazione molto più generale nel teorema 10.14.

Possiamo introdurre un ordine in $\mathbb{Q}$ che **estende** l'ordine di $\mathbb{Z}$. Si può dimostrare che tale ordine è *compatibile con le operazioni* di $\mathbb{Q}$, nel senso che per ogni

$$x, y, z \in \mathbb{Q}, \quad \text{con} \quad x \leq y, \quad \text{si ha} \quad x + z \leq y + z$$

$$\text{e se} \quad z > 0, \quad \text{si ha} \quad xz \leq yz.$$

Si può provare che l'ordine in $\mathbb{Z}$ non è denso, mentre l'ordine in $\mathbb{Q}$ è denso, cioè per $x < y$ in $\mathbb{Q}$ l'elemento $z = \frac{x+y}{2} \in \mathbb{Q}$ soddisfa $x < z < y$. Viceversa l'ordine di $\mathbb{Q}$ non è buono, infatti l'insieme dei numeri razionali positivi non ammette minimo e non è completo.

Un altro fatto sui numeri razionali di facile dimostrazione è il seguente. Al solito diremo che un numero $a \in \mathbb{Z}$ è *pari* se è della forma $a = 2b$ con $b \in \mathbb{Z}$. Per $a \in \mathbb{N}$ questa definizione coincide con quella già data per numeri naturali. Diremo che a è *dispari*, se non è pari. Non è difficile vedere che questo accade precisamente quando $a = 2n + 1$ per qualche $n \in \mathbb{Z}$. Usando l'esercizio 1.17 possiamo presentare ogni numero intero in modo unico come prodotto $2^m(2n + 1)$, dove $m \in \mathbb{N}$ e $n \in \mathbb{Z}$.

Proposizione 2.4. *Non esistono numeri razionali il cui quadrato è 2.*

DIMOSTRAZIONE. Supponiamo che esista un numero razionale r con $r^2 = 2$. Allora $r \neq 0$ e quindi possiamo scrivere $r = a/b$, dove a e b sono interi, non entrambi pari. Infatti, presentando a e b nella forma $2^m(2n + 1)$ possiamo semplificare la frazione per ottenere una frazione con la proprietà richiesta. Ora $(a/b)^2 = 2$ dà $a^2 = 2b^2$, di conseguenza a^2 è pari, e quindi anche a è pari. Sia $a = 2a_1$, con un intero a_1. Allora $4a_1^2 = 2b^2$. Di conseguenza $2a_1^2 = b^2$, e quindi b^2 è pari. Questo implica che anche b è pari, assurdo. □

I numeri reali $\mathbb{R}$ sono già stati introdotti nei corsi di analisi. Osserviamo solamente che anche in $\mathbb{R}$ sono definite le operazioni di addizione, moltiplicazione e un ordinamento. Supponiamo noto il fatto che si possa immaginare $\mathbb{Q}$ come un sottoinsieme di $\mathbb{R}$. Una delle proprietà importanti di $\mathbb{R}$ è la completezza.

Tra le altre proprietà di $\mathbb{R}$, citiamo le seguenti:

(a) $\mathbb{Q}$ è denso in $\mathbb{R}$, cioè se $x, y \in \mathbb{R}$ e $x < y$, allora esiste $z \in \mathbb{Q}$ tale che $x < z < y$;
(b) ogni numero reale è l'estremo superiore di un insieme di numeri razionali;
(c) ogni numero reale non negativo è un quadrato, cioè per ogni $a \in \mathbb{R}$, $a \geq 0$, esiste $b \in \mathbb{R}$ tale che $b^2 = a$.

Il seguente lemma dà un'idea di come si potrebbe dimostrare il punto (a).

Lemma 2.5. *Per ogni numero reale ρ, esiste un numero intero $n \geq \rho$.*

DIMOSTRAZIONE. Ragioniamo per assurdo e supponiamo che per qualche numero reale ρ si abbia $n < \rho$ per ogni $n \in \mathbb{Z}$. Quindi l'insieme $\mathbb{Z}$ è superiormente limitato. Sia σ l'estremo superiore di $\mathbb{Z}$, allora $\sigma - 1$, essendo minore di σ non è più un limite superiore per $\mathbb{Z}$, pertanto $\sigma - 1 \leq n$ per qualche $n \in \mathbb{Z}$ e quindi $\sigma \leq n + 1$, assurdo poiché σ è un limite superiore per $\mathbb{Z}$. □

Definizione 2.6. Per ogni numero reale ρ denotiamo con $\lfloor \rho \rfloor$ l'unico numero intero n determinato da $n \leq \rho < n+1$ e lo chiamiamo *parte intera*. Per il lemma 2.5, questa definizione è sensata.

La proposizione 2.4 e l'esempio 1.76 permettono di asserire che l'insieme $\mathbb{Q}$ è strettamente contenuto in $\mathbb{R}$. Gli elementi dell'insieme $\mathbb{R} \setminus \mathbb{Q}$ si dicono *numeri irrazionali*.

2.3 I numeri complessi

Nell'insieme delle coppie ordinate dei numeri reali $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ definiamo due operazioni di addizione e moltiplicazione ponendo per ogni coppia di elementi $z = (a, b), z' = (a', b') \in \mathbb{C}$:

$$z + z' = (a + a', b + b'), \quad z \cdot z' = (aa' - bb', ab' + ba'),$$

Per ogni $z = (a, b), z' = (a', b'), z'' = (a'', b'') \in \mathbb{C}$, valgono le seguenti proprietà, la cui dimostrazione lasciamo per esercizio:

A1. $z + (z' + z'') = (z + z') + z''$ (associatività dell'addizione);
A2. $z + z' = z' + z$ (commutatività dell'addizione);
A3. $z + (0, 0) = z$ (elemento neutro dell'addizione);
A4. $(a, b) + (-a, -b) = (0, 0)$ (opposto);
M1. $z \cdot (z' \cdot z'') = (z \cdot z') \cdot z''$ (associatività della moltiplicazione);
M2. $z \cdot z' = z \cdot z'$ (commutatività della moltiplicazione);
M3. $z \cdot (1, 0) = z$ (elemento neutro della moltiplicazione);
M4. se $z \neq 0$, $(a, b) \cdot (a/(a^2 + b^2), -b/(a^2 + b^2)) = (1, 0)$ (inverso);
D1. $z \cdot (z' + z'') = z \cdot z' + z \cdot z''$ (distributività della moltiplicazione rispetto all'addizione).

Allora $\mathbb{C}$ con queste due operazioni risulta essere un campo, come dalla definizione 4.16, che chiameremo il *campo complesso* e definiamo i suoi elementi *numeri complessi*.

L'applicazione $j : \mathbb{R} \longrightarrow \mathbb{C}$ tale che $j(a) = (a, 0)$ è un'applicazione iniettiva che conserva le somme e i prodotti. Questo permette di identificare i numeri reali con i numeri complessi della forma $(a, 0)$ e di pensare ad $\mathbb{R}$ come a un sottoinsieme (sottocampo) di $\mathbb{C}$.

Denotiamo con i l'elemento $(0, 1)$ di $\mathbb{C}$ e lo chiamiamo *unità immaginaria*. Osserviamo che $i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1$, in base all'identificazione appena vista. Quindi i è una radice quadrata di -1.

Ora ogni numero complesso si può scrivere nella forma seguente, utilizzando l'identificazione di $\mathbb{R}$ in $\mathbb{C}$

$$z = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + bi.$$

In questo modo a si dice la *parte reale di* z e si denota $a = Re(z)$ e $b = Im(z)$ si dice la *parte immaginaria di* z. Con questa nuova notazione, risulterà più comodo operare utilizzando le usuali regole del calcolo letterale, ricordando che si ha $i^2 = -1$.

Esempio 2.7. $(1+i\sqrt{2})(7-i) = (7+\sqrt{2}) + i(-1+7\sqrt{2})$,

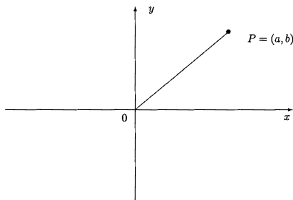
$$\frac{1+i3}{4-i\sqrt{2}} = \frac{(1+i3)(4+i\sqrt{2})}{(4-i\sqrt{2})(4+i\sqrt{2})} = \frac{4-3\sqrt{2}}{18} + i\frac{12+\sqrt{2}}{18}.$$

Definiamo il *coniugato* di un elemento $z = a + ib$ come $\overline{z} = a - ib$. L'applicazione che manda un elemento di $\mathbb{C}$ nel suo coniugato si dice *coniugazione* ed è un'applicazione che conserva le somme e i prodotti. Infatti

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \qquad \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}, \qquad \overline{\overline{z}} = z.$$

L'ultima uguaglianza prova che la coniugazione è un'applicazione involutoria, pertanto è biettiva e la sua inversa coincide con la coniugazione stessa. Valgono inoltre le seguenti proprietà:

$$z+\overline{z} = 2Re(z) \in \mathbb{R}; \qquad z-\overline{z} = 2iIm(z) \in i\mathbb{R}; \qquad z\cdot\overline{z} = a^2+b^2 \in \mathbb{R}.$$

Fissiamo ora un sistema di coordinate cartesiane ortogonali x, y su un piano che chiameremo *piano di Argand-Gauss*. Ogni numero complesso $a + ib$ si può rappresentare geometricamente con il punto P di coordinate (a, b). Questa assegnazione dà luogo ad una corrispondenza biunivoca tra i punti del piano di Gauss e i numeri complessi.

L'asse x è detto *asse reale* e l'asse y è detto *asse immaginario*. La distanza di $P = (a, b)$ dall'origine, cioè il numero reale non negativo $\rho = \sqrt{a^2 + b^2}$ è detto il *modulo* del numero complesso $z = a+ib$ e viene denotato con $|z|$. Il numero reale φ che misura l'angolo orientato formato dal semiasse positivo delle x e dalla semiretta

di origine 0 e passante per P viene detto *argomento* o *anomalia* di $z = a + ib$. Osserviamo che φ non è determinato se $P = (0,0)$, cioè se $z = 0$. Concludiamo che un numero complesso diverso da zero individua univocamente il proprio modulo, ma determina il proprio argomento solo a meno di multipli interi di 2π. Osserviamo che $|z| = \sqrt{z \cdot \overline{z}}$ e quindi l'inverso del numero complesso z è

$$z^{-1} = \frac{\overline{z}}{|z|^2}.$$

Dalla definizione di seno e coseno si ha

$$a = \rho\ \cos\varphi, \quad b = \rho\ \operatorname{sen}\varphi, \quad z = \rho(\cos\varphi + i\operatorname{sen}\varphi).$$

Questa è la *forma trigonometrica* del numero complesso z.

La scrittura in forma trigonometrica è molto utile per calcolare il prodotto di due numeri complessi $z = \rho(\cos\varphi + i\operatorname{sen}\varphi)$ e $z' = \rho'(\cos\varphi' + i\operatorname{sen}\varphi')$.

$$\begin{aligned} z \cdot z' &= \rho(\cos\varphi + i\operatorname{sen}\varphi)\rho'(\cos\varphi' + i\operatorname{sen}\varphi') = \\ &= (\rho\rho')[(\cos\varphi\cos\varphi' - \operatorname{sen}\varphi\operatorname{sen}\varphi') + i(\cos\varphi\operatorname{sen}\varphi' + \operatorname{sen}\varphi\cos\varphi')] = \\ &= (\rho\rho')(\cos(\varphi+\varphi') + i\operatorname{sen}(\varphi+\varphi')). \end{aligned}$$

Pertanto abbiamo provato il seguente lemma.

Lemma 2.8. *Il prodotto di due numeri complessi ha per modulo il prodotto dei moduli e per argomento la somma degli argomenti.*

Questo semplice calcolo ha come corollario una formula che si rivelerà molto utile.

Corollario 2.9. (Formula di De Moivre) *Se $z = \rho(\cos\varphi + i\operatorname{sen}\varphi)$ è un numero complesso scritto in forma trigonometrica, e $n \in \mathbb{N}$, allora*

$$z^n = \rho^n(\cos n\varphi + i\operatorname{sen} n\varphi).$$

DIMOSTRAZIONE. La dimostrazione è per induzione su n e utilizza la formula del prodotto di due numeri complessi. □

Una conseguenza della formula di De Moivre è il calcolo delle soluzioni dell'equazione in $x^n = w$, con $w \in \mathbb{C}$. Infatti z è soluzione di quest'equazione, e si dice che z è *radice n-esima* di w se e solo se $z^n = w$. Pertanto se $0 \neq z = \rho(\cos\varphi + isen\varphi)$ e $0 \neq w = \tau(\cos\vartheta + isen\vartheta)$, dalla formula di De Moivre si deduce

$$\rho = \sqrt[n]{\tau} \qquad \varphi = (\vartheta + 2k\pi)/n, \quad k \in \mathbb{Z}.$$

Pertanto se

$$z_k = \sqrt[n]{\tau}\left(\cos\left(\frac{\vartheta + 2k\pi}{n}\right) + i\operatorname{sen}\left(\frac{\vartheta + 2k\pi}{n}\right)\right)$$

si ha che z_k è una radice n-esima di w per ogni $k \in \mathbb{Z}$. Sia ora $k \in \mathbb{Z}$, facciamo la divisione con il resto tra k ed n. (Daremo una dimostrazione dell'esistenza del quoziente e del resto nella divisione di k per n nel teorema 3.6). Otteniamo quindi $k = qn + r$, con $0 \leq r \leq n - 1$ e quindi $z_k = z_r$. Inoltre $z_k = z_h$ se e solo se $k - h = nt$ con $t \in \mathbb{Z}$. Pertanto $z_0, z_1, z_2, \dots, z_{n-1}$ sono tutte le radici distinte di w. Abbiamo così provato il seguente lemma.

Lemma 2.10. *Ogni numero complesso $w \neq 0$ ammette n radici n-esime distinte, per ogni $0 \neq n \in \mathbb{N}$. Esse sono rappresentate nel piano di Argand-Gauss dai vertici di un poligono regolare di n lati inscritto nella circonferenza di centro 0 e raggio $\sqrt[n]{|w|}$, ed avente un vertice in $(1, 0)$.*

Osserviamo infine che $w = 0$ ha un'unica radice n-esima $z = 0$. Riscriviamo il lemma 2.10 nel caso particolare in cui $w = 1$.

Corollario 2.11. *Le n radici complesse n-esime dell'unità sono*

$$\omega_k = \cos(2k\pi/n) + i \operatorname{sen}(2k\pi/n), \quad per \quad k = 0, 1, \dots, n-1.$$

Vediamo alcuni esempi.

Esempio 2.12. Calcoliamo $(1+i)^6 = (\sqrt{2}(1/\sqrt{2} + i/\sqrt{2}))^6$:

$$(1+i)^6 = [\sqrt{2}(\cos(\pi/4) + i \operatorname{sen}(\pi/4))]^6 = 8(\cos(6\pi/4) + i \operatorname{sen}(6\pi/4) = 8i.$$

Analogamente si conclude, osservando che $(1+i)^2 = 2i$.

Se vogliamo calcolare $(1-i)^{179}$, poniamo $a = 1-i$, allora $a^2 = -2i$ e $a^4 = -4$. Pertanto

$$a^{179} = a^{4 \cdot 44} \cdot a^2 \cdot a = (-4)^{44} \cdot (-2i) \cdot (1-i) = -2^{89}(1+i).$$

Esempio 2.13. Calcoliamo le soluzioni dell'equazione $x^3 - 2i = 0$.

Sia $z = \rho(\cos\varphi + i \operatorname{sen}\varphi) \in \mathbb{C}$ soluzione dell'equazione $x^3 = 2i$. Allora

$$\rho^3 = 2, \quad 3\varphi = \pi/2 + 2k\pi \implies \rho = \sqrt[3]{2}, \quad \varphi = \pi/6 + 2k\pi/3.$$

Si deduce che le tre soluzioni sono

$$z_0 = \sqrt[3]{2}\left(\frac{\sqrt{3}}{2} + \frac{i}{2}\right), \quad z_1 = \sqrt[3]{2}\left(-\frac{\sqrt{3}}{2} + \frac{i}{2}\right) \quad \text{e} \quad z_2 = -\sqrt[3]{2}i.$$

Esempio 2.14. Le radici quarte dell'unità sono $i, -1, -i, 1$.

2.4 Interpretazione geometrica delle operazioni tra numeri complessi

Ci sono facili interpretazioni geometriche di tutte e tre le operazioni tra numeri complessi.

L'addizione corrisponde alla *traslazione*. Infatti il punto $z + b$ si ottiene dal punto z tramite la traslazione definita dal vettore con inizio l'origine 0 e con punto finale il punto rappresentato da b.

Se a è un numero complesso con $|a| = 1$, allora la moltiplicazione per a corrisponde alla rotazione in senso antiorario e con centro 0 di un angolo φ uguale all'argomento di a. Se invece $r = |a|$ è arbitrario, ma non nullo, allora la moltiplicazione per a corrisponde alla rotazione di centro 0 ed angolo φ, seguita dalla dilatazione di centro 0 e coefficiente r.

La coniugazione corrisponde alla simmetria di asse x.

La retta definita dall'origine e dal punto z è precisamente il luogo determinato da tutti i numeri complessi del tipo λz, dove $\lambda \in \mathbb{R}$. I punti del segmento $[0, z]$ sono ottenuti con $0 \leq \lambda \leq 1$, mentre quelli della semiretta con inizio z che non contiene l'origine 0, con $\lambda \geq 1$ e quelli della semiretta con inizio 0 che non contiene z, con $\lambda \leq 0$. Il punto medio del segmento $[0, z]$ è proprio $\frac{1}{2}z$.

Diamo un'altra utile applicazione dei numeri complessi. È comodo rappresentare un insieme finito ordinato sul piano di Argand-Gauss nel modo seguente. Sia $(X, \leq)$ un insieme dotato di preordine. Se $a, b \in X$ vengono rappresentati da α e β sul piano di Argand-Gauss, allora $a < b$ se e solo se $\alpha \prec \beta$, ove $\prec$ è la relazione d'ordine definita sui complessi come nel punto (a) dell'esercizio 2.27. Se uniamo con una linea i punti tra loro confrontabili, otteniamo un diagramma nel piano, noto come il *diagramma di Hasse*. Osserviamo inoltre che, per rendere meno pesante il diagramma, ogni qualvolta si ha $a < b < c$, essendo la relazione transitiva, si omette di disegnare la linea che collega a con c.

Ad esempio, se consideriamo l'insieme $X = \{a, b, c\}$ e la relazione d'ordine definita su $\mathcal{P}(X)$ come nel punto (a) dell'esempio 1.54, otteniamo il seguente diagramma:

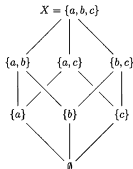



Diagramma di Hasse di $P(\{a, b, c\})$

2.5 Esercizi sui numeri

Esercizio 2.1 Dimostrare che $\bigcap_{n=1}^{\infty}]n, +\infty[= \emptyset$.

Esercizio 2.2 Si provi che $\bigcap_{n=1}^{\infty}] -\frac{1}{n}, +\frac{1}{n}[= \{0\}$.

Esercizio 2.3 Sia α un numero reale irrazionale e sia $n \in \mathbb{N}_+$. Allora esistono $m, k \in \mathbb{Z}$ tali che $|m\alpha - k| < \frac{1}{n}$. Inoltre m può essere scelto con $0 < m < n$.

Esercizio 2.4 Siano α e β due numeri complessi con $\alpha^2 = \beta^3 = (\alpha \cdot \beta)^7 = 1$. Dedurre che $\alpha = \beta = 1$.

Esercizio 2.5 Siano z_1 e z_2 due punti distinti del piano di Argand-Gauss. Determinare i numeri complessi che corrispondono ai punti della retta che passa per z_1 e z_2.

Esercizio 2.6 Siano z_1 e z_2 due punti distinti del piano di Argand-Gauss. Dimostrare che il punto medio del segmento $[z_1, z_2]$ corrisponde al punto $\frac{z_1+z_2}{2}$.

Esercizio 2.7 Dimostrare che le tre mediane di un triangolo si intersecano in un solo punto che le divide in rapporto 2 : 1.

Esercizio 2.8 Dimostrare che quattro punti a, b, c, d del piano di Argand-Gauss formano un parallelogramma se e solo se $a + c = b + d$.

Esercizio 2.9 Dimostrare che i punti medi dei quattro lati di un quadrangolo formano un parallelogramma.

Esercizio 2.10 Dimostrare che i punti medi di due lati opposti di un quadrangolo e i punti medi delle sue diagonali formano un parallelogramma.

Esercizio 2.11 Siano a e b due punti del piano di Argand-Gauss. Dimostrare che l'area del trianglo determinato da a, b e l'origine coincide con $\frac{1}{4}|b\bar{a} - a\bar{b}|$.

Esercizio 2.12 Esprimere nella forma $x + iy$ i seguenti numeri complessi

$$\frac{7-6i}{2+3i}, \quad \frac{2i}{(2+i)^2}.$$

Esercizio 2.13 Si scrivano in forma trigonometrica i seguenti numeri complessi

$$\frac{2-2i}{3+3i}, \quad -7\sqrt{3}, \quad (1+i\sqrt{3})^2.$$

Esercizio 2.14 Si determinino tutte le soluzioni complesse $z \in \mathbb{C}$ del sistema:

$$\begin{cases} |z| = 1 \\ |1-z| = 1. \end{cases}$$

Esercizio 2.15 Si calcolino

$$(1+i)^{86},\ (1+i\sqrt{3})^{42},\ (\sqrt{3}-i)^{210},\ (1-i)^{79}.$$

Esercizio 2.16 Sia $z = \rho(\cos(\varphi) + i\,\mathrm{sen}(\varphi)) \in \mathbb{C}$. Si scrivano in forma trigonometrica $\bar{z}$ e z^{-1}.

Esercizio 2.17 Si calcolino e si disegnino sul piano di Argand-Gauss le soluzioni in $\mathbb{C}$ dell'equazione $x^4 + i = 0$.

Esercizio 2.18 Si calcolino $(1-i)^{28}, i^{-1}$.

Esercizio 2.19 Si scrivano in forma trigonometrica i seguenti numeri complessi $3\sqrt{5}i, 5-5i$.

Esercizio 2.20 Esprimere nella forma $x + iy$ i seguenti numeri complessi

$$\frac{1-3i}{3-4i},\quad \frac{(2-\sqrt{5}i)^2}{3i}.$$

Esercizio 2.21 Sia z un numero complesso. Si dimostri che vale

$$-|z| \leq Re(z) \leq |z| \quad \text{e} \quad -|z| \leq Im(z) \leq |z|.$$

Si deduca che per ogni coppia di numeri complessi $z_1, z_2 \in \mathbb{C}$ valgono:

$$|z_1 + z_2| \leq |z_1| + |z_2| \qquad \text{e} \qquad |z_1| - |z_2| \leq |z_1 - z_2|.$$

Esercizio 2.22 Dimostrare che per ogni numero naturale $n \geq 1$ risultano:

(a)

$$\binom{4n}{1} + \binom{4n}{5} + \binom{4n}{9} + \ldots + \binom{4n}{4n-3} =$$
$$= \binom{4n}{3} + \binom{4n}{7} + \binom{4n}{11} + \ldots + \binom{4n}{4n-1};$$

(b)

$$1 + \binom{12n+6}{4} + \binom{12n+6}{8} + \binom{12n+6}{12} + \ldots + \binom{12n+6}{12n+4} =$$
$$= \binom{12n+6}{2} + \binom{12n+6}{6} + \binom{12n+6}{10} + \ldots + \binom{12n+6}{12n+6}.$$

Esercizio 2.23 Si considerino le relazioni binarie R_1, R_2, R_3 e R_4 nell'insieme $\mathbb{C}$ dei numeri complessi definite come segue:

(a) xR_1y se il numero $x - y$ è naturale;
(b) xR_2y se il numero $x - y$ è razionale;
(c) xR_3y se il numero $x - y$ è reale e $x - y \geq 0$;

(d) xR_4y se la parte reale e la parte immaginaria del numero $x - y$ sono ≥ 0.

Si determini quali delle relazioni R_1, R_2, R_3 e R_4 sono relazioni di equivalenza, e quali sono ordini o preordini, specificando il tipo di ordine (buon ordine, ordine lineare ecc.).

Esercizio 2.24 Siano A e B gli insiemi dei divisori di 36 e 60, rispettivamente, ordinati per divisibilità. Si disegnino i diagrammi di Hasse di A e B.

Esercizio 2.25 Trovare il numero di tutti gli ordini di un insieme di 3 elementi.

Esercizio 2.26 Trovare il numero di tutti gli ordini di un insieme di 4 elementi.

Esercizio 2.27 Dimostrare che:

(a) la relazione $a \preceq b$ in $\mathbb{C}$ definita da $a \preceq b$ se e solo se Im $a \leq$ Im b è una relazione di preordine.
(b) la relazione $a \preceq_r b$ in $\mathbb{C}$ definita da $a \preceq_r b$ se e solo se Re $a \leq$ Re b è una relazione di preordine.

3

L'aritmetica dei numeri interi

Il primo paragrafo introduce i numeri primi e alcuni modi per generarli: il crivello di Eratostene e i polinomi di Eulero.

Nel secondo e terzo paragrafo si introducono la divisione con resto e l'algoritmo di divisione di Euclide che permette di trovare effettivamente il massimo comune divisore di due numeri interi. Il teorema di fattorizzazione in numeri primi, noto anche come teorema fondamentale dell'aritmetica, viene dimostrato nel quarto paragrafo. Nel quinto e sesto paragrafo vengono introdotte le congruenze modulo m in $\mathbb{Z}$, le equazioni congruenziali e qualche esempio di equazione diofantea. Nel settimo si dimostrano alcuni criteri di divisibilità negli interi.

L'ottavo paragrafo è dedicato al teorema di Fermat, mentre nel paragrafo successivo studiamo la funzione di Eulero e dimostriamo il teorema di Eulero che generalizza il teorema di Fermat. Nei paragrafi 10, 11 12 e 13 raccogliamo ulteriori proprietà dei numeri primi: cenni sui generatori di numeri primi (i numeri primi di Fermat e di Mersenne) e sulla distribuzione dei numeri primi e infine la descrizione dei numeri che si possono scrivere come somma di due quadrati.

3.1 I numeri primi

Abbiamo introdotto nel paragrafo 2.1 l'insieme dei numeri interi

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}.$$

Ricordiamo che abbiamo definito in $\mathbb{Z}$ l'addizione e la moltiplicazione che godono delle proprietà descritte nei lemmi 2.1, 2.2 e 2.3. Ricordiamo inoltre la relazione di $\leq$ (*minore o uguale di*) definita su $\mathbb{Z}$, in base alla quale $\mathbb{Z}$ viene ordinato linearmente. Vogliamo ora introdurre un'altra relazione in $\mathbb{Z}$.

La divisione in $\mathbb{Z}$. Dati due numeri interi m ed n si dice che m *divide* n o anche che m *è divisore di* n se esiste $c \in \mathbb{Z}$ tale che $n = mc$. In tal caso scriviamo $m|n$. Si ha:

(a) $m|0$ per ogni $m \in \mathbb{Z}$, mentre $0|m$ solo per $m = 0$;

(b) $\pm 1 | n$ e $\pm n | n$ per ogni $n \in \mathbb{Z}$.

Allora "m divide n" definisce una relazione binaria in $\mathbb{Z}$. Se $m|n$ e $n|m$ diremo che *m è associato a n* e denotiamo con $\sim$ la relazione "essere associato". È facile vedere che $\sim$ è una relazione di equivalenza in $\mathbb{Z}$. L'insieme $\{1, -1\}$ coincide con la classe di equivalenza di 1. Più in generale, la classe di equivalenza di $m \in \mathbb{Z}$ coincide con $\{m, -m\}$, cioè $n \sim m$ se e solo se $n = \pm m$. Poiché ogni $n \in \mathbb{Z}$ ha come divisori ± 1 e $\pm n$, questi divisori sono chiamati *divisori impropri* di n. Un divisore m di n si dice *proprio* se non è improprio, cioè $m \neq \pm 1, \pm n$.

Denoteremo con $\mathbb{Z}^*$ l'insieme dei numeri interi non nulli.

Definizione 3.1. Un numero $b \in \mathbb{Z}^*$ si dice *primo*, se $p \neq \pm 1$ e p non ha divisori propri.

I numeri primi servono come "atomi" dai quali si possono ottenere, in modo unico, tutti gli altri numeri di $\mathbb{Z}$ tramite moltiplicazioni. È chiaro che un numero intero $m > 1$ non è primo se e solo se $m = ab$ con $1 < a < m$.

Il seguente metodo, detto *crivello di Eratostene*, consente di determinare i numeri primi minori di un numero assegnato n. Vediamo un esempio con n ragionevolmente piccolo, $n = 40$. Scriviamo in ordine tutti gli interi da 2 a 40. Il primo intero 2 risulta primo non potendo avere dei divisori propri < 2 nella lista. Mettiamolo nella lista dei primi e cancelliamo poi con un tratto / di penna tutti i numeri pari > 2, cioè i multipli di 2 maggiori di 2. Il primo intero che rimane è 3, che risulta primo per lo stesso motivo di 2. Aggiungiamo 3 alla lista dei numeri primi e cancelliamo con un tratto \ di penna tutti i numeri multipli di 3. Il più piccolo intero che rimane, 5, è primo. Aggiungiamo 5 alla lista, cancelliamo poi con un tratto — di penna tutti i numeri multipli di 5 e così via.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~
~~28~~ 29 ~~30~~ 31 ~~32~~, ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~

Così i primi minori di 40 risultano essere $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ e 37.

Per determinare se un numero $a > 0$ è primo si può controllare se è divisibile per qualche primo minore di a. In realtà basta verificarlo su un insieme più piccolo, come si descrive nell'esercizio 3.3.

Osserviamo inoltre che il crivello di Eratostene permette di dire, al passo corrispondente a p, quali sono i numeri primi fino a $(p+2)^2 - 1$, se p è un numero primo dispari, si veda l'esercizio 3.3. Quindi, per esempio, considerando solo i primi minori o uguali a 31, si possono calcolare tutti i primi minori di 1000. Ci si può quindi chiedere se questo procedimento può terminare dopo un numero finito di passi, ed ottenere quindi tutti i numeri primi. Il teorema 3.13 darà la risposta.

Quello che abbiamo fatto finora è stato di capire se certi numeri interi sono primi o no. Ci sono anche dei metodi per "costruire" numeri primi, ad esempio nell'esercizio 3.4 che è un caso particolare di una definizione più generale che vedremo più avanti nell'esercizio 3.19. Si può dimostrare che non esiste alcun polinomio $f(x)$ con coefficienti interi, tale che tutti i valori $f(x)$ per $x \geq x_0$, intero, siano primi. Tuttavia esistono delle funzioni più complesse che danno come valori solo numeri primi. Per

esempio, è noto che esiste una costante positiva A tale che per ogni numero naturale x il valore $\lfloor A^{3^x} \rfloor$ è un numero primo. È molto più facile trovare invece dei polinomi che danno come valori solamente numeri composti, come per esempio $n^4 + 4$. Infatti $n^4 + 4$ è composto per ogni $n \in \mathbb{Z}$, essendo $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$, il cosiddetto *teorema di Sophie Germain*.

3.2 Massimo comun divisore e minimo comune multiplo

Definizione 3.2. Un *massimo comun divisore* d dei numeri interi a e b, con $a, b \in \mathbb{Z}$ non entrambi nulli, è definito come un divisore comune di a e b, cioè $d|a$ e $d|b$, per il quale risulti $d'|d$ per ogni altro divisore comune d' di a e b.

Se d è un massimo comun divisore di a e b, lo è anche $-d$. Quindi il massimo comun divisore è determinato solo a meno del segno. Infatti se d_1 e d_2 sono massimi comun divisori di a e b, si ha $d_1 = \pm d_2$. Tuttavia spesso prendiamo in considerazione il massimo comun divisore *positivo* (a, b) di a e b, che coincide anche con il più grande di tutti i divisori comuni di a e b. Diremo che a e b *sono coprimi* se $(a, b) = 1$.

Definizione 3.3. Il *minimo comune multiplo* m dei numeri interi a e b è definito come un multiplo comune di a e b, cioè $a|m$ e $b|m$, per il quale risulta $m|m'$ per ogni altro multiplo comune m' di a e b.

Se m è minimo comune multiplo di a e b, lo è anche $-m$. Quindi il minimo comune multiplo è determinato solo a meno del segno. Tuttavia spesso prendiamo in considerazione il minimo comune multiplo *positivo* $m.c.m.(a, b)$ di a e b.

Vediamo ora alcune altre proprietà dei divisori e del massimo comun divisore.

Lemma 3.4. *(d_1) Se $c|a$ e $c|b$, allora $c|ka + mb$ per ogni scelta di $k, m \in \mathbb{Z}$.*
(d_2) Se $a|a'$ e $b|b'$, allora $ab|a'b'$.
(d_3) Se $d|a$, $d|b$ e $d = ka + mb$, allora d è un massimo comun divisore di a e b, cioè $d = \pm(a, b)$.
(d_4) Se $d = (a, b)$, allora $a = da_1$ e $b = db_1$, con $a_1, b_1 \in \mathbb{Z}$, coprimi.

DIMOSTRAZIONE. (d_1) Siano $a = cx$ e $b = cy$, con $x, y \in \mathbb{Z}$. Allora

$$ka + mb = c(kx + my),$$

quindi $c|ka + mb$.

(d_2) Se $a' = ax$ e $b' = by$, allora $a'b' = ab(xy)$.

(d_3) Sia d' un divisore comune di a e b. Allora $d'|d$ per il punto (d_1). Quindi d è massimo comun divisore di a e b.

(d_4) Sia $d' = (a_1, b_1)$. Allora $d'|a_1$ e $d'|b_1$, quindi $dd'|da_1 = a$ e $dd'|db_1 = b$ per il punto (d_2). Quindi dd' è un divisore comune di a e b. Dunque $dd'|d$. Poiché anche $d|dd'$, si conclude che $dd' = \pm d$, cioè $d' = 1$. □

Corollario 3.5. *Sia p primo. Se p non divide un numero intero a, allora p ed a sono coprimi.*

DIMOSTRAZIONE. Sia c un divisore comune di a e p. Poiché p è primo e p non divide a, gli unici divisori comuni di a e p sono ± 1. Pertanto c ed a sono coprimi. □

3.3 La divisione euclidea

Vedremo che una via per stabilire l'esistenza del massimo comun divisore è la proprietà che permette di eseguire la "divisone con resto", detta anche *divisone euclidea*, come descritto nel teorema 3.6. Introduciamo l'applicazione *valore assoluto* o *modulo* $|\ | : \mathbb{Z} \to \mathbb{N}$ definita da

$$|x| = \begin{cases} x \text{ se } x \geq 0, \\ -x \text{ se } x < 0. \end{cases}$$

Si osservi che $|x| = 0$ se e solo se $x = 0$. Valgono inoltre per ogni $x, y \in \mathbb{Z}$,

$$|x| + |y| \geq |x + y|; \qquad |x||y| = |xy|.$$

Teorema 3.6. *Se* $a, b \in \mathbb{Z}$ *e* $b \neq 0$, *esistono unici* $q, r \in \mathbb{Z}$ *tali che* $a = q \cdot b + r$ *e* $0 \leq r < |b|$.

DIMOSTRAZIONE. Si considera prima il caso $a \geq 0$ e $b > 0$. Procediamo per induzione su a. Notiamo prima che per ogni $0 \leq a < b$ possiamo prendere $q = 0$ e $r = a$. Se $a = b$ si prende semplicemente $q = 1$ e $r = 0$. Supponiamo ora $a > b$ e che tali q ed r si possano trovare per $a - 1$, cioè $a - 1 = qb + r$ con $q \in \mathbb{Z}$ e $0 \leq r < b$. Se $r < b - 1$, allora con $0 \leq r' = r + 1 < b$ abbiamo $a = aq + r'$. Se invece $r = b - 1$, allora $a = (q + 1)b$. Sia ora $a < 0$. Allora $-a > 0$ e pertanto esistono t ed s tali che $-a = bt + s$, con $0 \leq s < b$. Se $s = 0$, basta porre $q = -t$ ed $r = s = 0$. Se $s > 0$, osserviamo che $0 \leq b - s < b$, da cui, ponendo $q = -t - 1$ ed $r = b - s$, si ha

$$a = b(-t) - s = b(-t) - b + b - s = b(-t - 1) + (b - s) = bq + r.$$

Supponiamo ora $b < 0$. Allora $-b > 0$, $|-b| = |b|$ ed esistono $t, r \in \mathbb{Z}$, tali che $a = (-b)t + r$, con $0 \leq r < |b| = |-b|$. Basta porre $q = -t$ e si ha $a = bq + r$.
Verifichiamo l'unicità. Supponiamo esistano $q, q', r, r' \in \mathbb{Z}$ tali che

$$a = bq + r = bq' + r', \quad \text{con} \quad 0 \leq r, \ r' < |b|.$$

Supponiamo ad esempio che $r' \geq r$. Allora $0 \leq r' - r = b(q - q')$ e passando ai valori assoluti si ha $|b||q - q'| = |b(q - q')| = r' - r \leq r' < |b|$. Si ricava dunque $|q - q'| < 1$, cioè $q = q'$ e pertanto $r = r'$. □

La divisione con resto è rilevante per i numeri interi, ma non per $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, perché la divisibilità $b|a$ c'è sempre quando $b \neq 0$ poiché esiste l'inverso b^{-1} di b e quindi $a = b(b^{-1}a)$, in altre parole, essi sono *campi*.

Teorema 3.7. *Se $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$, allora esiste il massimo comun divisore d di a e b ed ha la forma $d = ua + vb$, con $u, v \in \mathbb{Z}$.*

DIMOSTRAZIONE. Consideriamo l'insieme

$$S = \{s : s = ax + by \text{ con } x, y \in \mathbb{Z}, s > 0\}.$$

Poiché $(a, b) \neq (0, 0)$, possiamo supporre per esempio $b \neq 0$. Allora se $b > 0$, $b \in S$, se $b < 0$, allora $b(-1) = -b \in S$. Ugualmente se $a \neq 0$. Quindi S è un sottoinsieme non vuoto di $\mathbb{N}$. Allora per il principio del minimo 1.58, S contiene un elemento minimo $d = au + bv$. Proviamo che risulta $d = (a, b)$. Per la divisione euclidea applicata ad a e d, esistono q ed r tali che $a = dq + r$, $0 \leq r < d$. Allora $r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq)$. Se supponiamo $r \neq 0$, allora $r > 0$, pertanto $r \in S$. La condizione $r < d$ contraddice la minimalità di d e forza dunque $r = 0$, cioè d divide a. Analogamente d divide b. Sia ora z un divisore comune di a e b. Allora per il lemma 3.4 (d_1) si conclude che z divide d. □

La dimostrazione del teorema non è costruttiva, cioè non spiega come trovare effettivamente il massimo comun divisore e la sua espressione come combinazione lineare $d = ua + vb$ a partire da a e b. Descriviamo un procedimento, noto come *algoritmo di Euclide*, che permette di farlo.

Per il teorema 3.6, esistono $q_1, r_1 \in \mathbb{Z}$ con $a = q_1 \cdot b + r_1$ e $r_1 < b$. Se $r_1 = 0$ abbiamo $b|a$ e quindi $d = b = 0 \cdot a + 1 \cdot b$.

Se $r_1 > 0$ possiamo continuare, esistono $q_2, r_2 \in \mathbb{Z}$ con $b = q_2 \cdot r_1 + r_2$ e $0 \leq r_2 < r_1$. Osserviamo che r_1 ed r_2 dividono [illegible], se non sono nulli. Se $r_2 > 0$ possiamo continuare, esistono $q_3, r_3 \in \mathbb{Z}$ con $r_1 = q_3 \cdot r_2 + r_3$ e $0 \leq r_3 < r_2$; e così via. Si costruiscono in questo modo due successioni di interi

$$q_1, q_2, \ldots, q_k, \ldots \quad \text{e} \quad b > r_1 > r_2 > \ldots > r_k > \ldots \tag{1}$$

tali che

$$r_{s-1} = q_{s+1} r_s + r_{s+1} \text{ e quindi } \quad r_{s+1} = -q_{s+1} r_s + r_{s-1}. \tag{2}$$

Notiamo che $r_1 = a - q_1 b$ è combinazione lineare di a e b con coefficienti interi. Supponiamo che $r_1, \ldots, r_s$ siano combinazioni lineari di a e b, cioè, per $i = 1, 2, \ldots, s$ esistono $A_i, B_i \in \mathbb{Z}$ tali che $r_i = A_i a + B_i b$. Allora da (2) ricaviamo

$$r_{s+1} = r_{s-1} - q_{s+1} r_s = A_{s+1} a + B_{s+1} b,$$

dove

$$A_{s+1} = A_{s-1} - q_{s+1} A_s \quad \text{e} \quad B_{s+1} = B_{s-1} - q_{s+1} B_s. \tag{3}$$

Chiaramente, la successione (1) degli r_k si ferma a 0 dopo al più b passi, cioè esiste k con $r_{k+1} = 0$. Allora $r_{k-1} = q_{k+1} r_k$, quindi $r_k | r_{k-1}$. Supponiamo $k > s > 1$ e $r_k | r_{s+1}$ e $r_k | r_s$, dimostreremo che allora r_k divide anche r_{s-1}. Infatti basta applicare (2), poiché $r_k | r_{s+1}$ e $r_k | r_s$ per ipotesi. Ora con $s = 2$ ricaviamo $r_k | r_3$ e $r_k | r_2$, da cui r_k divide r_1. Ma allora $r_k | b = q_2 \cdot r_1 + r_2$ e $r_k | a = q_1 \cdot b + r_1$. D'altra parte, $r_k = A_k a + B_k b$ come già visto sopra. Allora, per il punto (d_3) del lemma 3.4, r_k è massimo comun divisore di a e b.

Useremo questo algoritmo per trovare il massimo comun divisore d tra due numeri naturali a e b e la sua espressione come combinazione lineare di a e b. Per mantenere una traccia del calcolo dei coefficienti A_s, B_s, i resti r_s ed i dividendi q_s costruiamo una tabella a 3 colonne. Nella prima riga mettiamo $1, 0, a$ e nella seconda $0, 1, b$ e poi si costruisce una riga, conoscendo le due precedenti usando le relazioni (2) e (3).

1	0	a
0	1	b
...	...	...
A_{s-1}	B_{s-1}	r_{s-1}
A_s	B_s	r_s
A_{s+1}	B_{s+1}	r_{s+1}

Abbiamo già visto che ogni riga di questa tabella soddisfa $r_k = A_k a + B_k b$.

Poiché nell'ultima colonna i valori continuano a diminuire, tale tabella si concluderà con $r = 0$ e la penultima riga fornisce le informazioni richieste. Calcoliamo ad esempio $(156, 84)$.

1	0	156
0	1	84
1	-1	72
-1	2	12
7	-13	0

Allora si avrà $12 = (156, 84)$ e $12 = -1 \cdot 156 + 2 \cdot 84$.

Lemma 3.8. *Se $a, b, c \in \mathbb{Z}$, c ed a sono coprimi e c divide ab, allora c divide b.*

DIMOSTRAZIONE. Essendo $1 = (a, c)$, per il teorema 3.7 possiamo scrivere

$$1 = ua + vc \text{ con } u, v \in \mathbb{Z}.$$

Moltiplicando per b si trova $b = uab + vcb$. Poiché $c|ab$ e $c|c$, il punto (d_1) del lemma 3.4 implica $c|b$. □

Vediamo ora una caratterizzazione importante dei numeri primi, cioè un numero è primo se e solo se ogni qualvolta divide il prodotto di due numeri, in realtà divide già uno dei due numeri.

Proposizione 3.9. *Un numero intero $p \neq 0, \pm 1$ è primo se e solo se per ogni coppia $a, b \in \mathbb{Z}$ con $p|ab$, si ha $p|a$ o $p|b$.*

DIMOSTRAZIONE. Sia p primo e si supponga che $p|ab$. Se p non divide a, allora p ed a sono coprimi per il corollario 3.5. Quindi per il lemma 3.8, $p|ab$ implica $p|b$.

Supponiamo che p non sia primo. Allora esistono dei divisori propri a e b di p con $p = ab$. In tal caso p non divide né a né b, ma p divide ab. □

Il minimo comune multiplo può essere definito anche utilizzando la definizione del massimo comun divisore.

Teorema 3.10. *Se $a, b \in \mathbb{Z}^*$ e d è un massimo comun divisore di a e b, allora $m = \frac{ab}{d}$ è un minimo comune multiplo di a e b.*

DIMOSTRAZIONE. Per il punto (d_4) del lemma 3.4 possiamo scrivere $a = da_1$ e $b = db_1$, con $a_1, b_1 \in \mathbb{Z}$, coprimi. Allora $m = a_1 b = b_1 a$ risulta un multiplo comune di a e b. Sia m' un altro multiplo comune di a e b. Allora da $a|m'$ e $b|m'$ si deduce $m' = ax$ e $m' = by$ con $x, y \in \mathbb{Z}$. Quindi $ax = by$ e di conseguenza $da_1 x = db_1 y$. Cancellando $d \neq 0$ si ha

$$a_1 x = b_1 y.$$

Per il lemma 3.8 e $(a_1, b_1) = 1$ possiamo concludere $a_1|y$ e $b_1|x$. Dunque $y = a_1 y_1$ e $x = b_1 x_1$per opportuni $x_1, y_1 \in \mathbb{Z}$. Pertanto $m' = ax = ab_1 x_1 = mx_1$ e quindi $m|m'$. □

Corollario 3.11. *Se a e b sono coprimi, allora $m.c.m.(a, b) = |ab|$. In particolare, se $a|c$ e $b|c$, e a e b sono coprimi, allora anche $ab|c$.*

3.4 Il teorema fondamentale dell'aritmetica

In questo paragrafo enunciamo e dimostriamo il *teorema fondamentale dell'aritmetica* che garantisce la fattorizzazione unica in prodotto di numeri primi nel senso seguente. Per ogni intero $a \neq 0, \pm 1$, esistono primi $p_1, \dots, p_k$ tali che

$$a = p_1 \dots p_k.$$

Inoltre se $p_1 \dots p_k = q_1 \dots q_s$ con $q_1, \dots, q_s$ numeri primi, allora $s = k$ e dopo una permutazione opportuna dei primi $p_1, \dots, p_k$ si ha $p_1 = \pm q_1, \dots, p_k = \pm q_k$.

Teorema 3.12. (Teorema fondamentale dell'aritmetica) *Tutti i numeri non invertibili di $\mathbb{Z}^*$ hanno una fattorizzazione unica in prodotto di numeri primi.*

DIMOSTRAZIONE. Per un numero intero $a \neq 0, \pm 1$ dimostriamo che a ha una fattorizzazione unica in prodotto di numeri primi. Basta considerare il caso $a > 0$. Ragioniamo per induzione su a. Il caso $a = 2$ è banale perché 2 è primo. Supponiamo $a > 2$. Se a è primo, abbiamo finito. Altrimenti esistono b e c in $\mathbb{Z}$ con $a = bc$ e $1 < b < a$, $1 < c < a$. Per l'ipotesi induttiva, entrambi b e c, essendo maggiori di 1, sono prodotti di numeri primi. Così abbiamo dimostrato l'esistenza della fattorizzazione di a in prodotto di numeri primi.

Per dimostrare l'unicità supponiamo che $a = p_1 \dots p_n = q_1 \dots q_s$ siano due fattorizzazioni di a in prodotto di numeri primi. Ragioniamo per induzione su n. Se

$n = 1$, avremo $p_1 = q_1 \dots q_s$, che implica $s = 1$ poiché p_1 è primo. Supponiamo ora $n > 1$. Allora p_1 divide il prodotto $q_1 \dots q_s$ e quindi divide uno dei fattori, diciamo q_1. Poiché q_1 è primo, concludiamo che $q_1 = \pm p_1$. Dopo la cancellazione abbiamo $p_2 \dots p_n = \pm q_2 \dots q_s$. Poiché l'elemento $a' = p_2 \dots p_n$ è prodotto di un numero di primi inferiore ad n, l'ipotesi induttiva garantisce che la sua fattorizzazione deve essere unica a meno di permutazione dei fattori, cioè si può supporre

$$s = n \text{ e } q_2 = \pm p_2, \; \dots, \; q_s = \pm p_n.$$

□

Sia $a > 1$, allora il teorema fondamentale dell'aritmetica permette di scrivere $a = p_1^{k_1} \dots p_s^{k_s}$, con $p_1, \dots, p_s$ numeri primi distinti. In questa forma l'unicità della fattorizzazione si può esprimere così: se $a = q_1^{m_1} \dots q_t^{m_t}$ è un'altra fattorizzazione di a, con $q_1, \dots, q_t$ numeri primi distinti, allora $t = s$, esiste un'opportuna permutazione dei primi $p_1, p_2, \dots, p_s$ con $q_1 = \pm p_1, \dots, q_s = \pm p_s$ e $m_1 = k_1, \dots, m_s = k_s$. Poiché $a > 0$, possiamo considerare fattorizzazioni con $p_i > 0$ e $q_j > 0$, perciò avremo $q_1 = p_1, \dots, q_s = p_s$, in altre parole, gli insiemi dei primi $\{p_1, \dots, p_s\}$ e $\{q_1, \dots, q_t\}$ coincidono, da cui $t = s$ e dopo un'eventuale riordino dei primi, per esempio in ordine crescente, coincidono le s-uple $(p_1, \dots, p_s)$ e $(q_1, \dots, q_s)$ e le s-uple $(m_1, \dots, m_s)$ e $(k_1, \dots, k_s)$.

Tuttavia in certe situazioni converrà usare anche fattorizzazioni $a = p_1^{k_1} \dots p_s^{k_s}$, con $p_1, \dots, p_s$ numeri primi distinti, permettendo di avere anche $k_i = 0$ per alcuni $i = 1, 2, \dots, s$. Questo risulta utile quando si lavora con più numeri $a, b, c, \dots$ per permettere un confronto tra loro. Scriviamo così

$$a = p_1^{k_1} \dots p_s^{k_s}, \quad b = p_1^{m_1} \dots p_s^{m_s} \quad \text{e} \quad c = p_1^{l_1} \dots p_s^{l_s}$$

dove $p_1, \dots, p_s$ sono numeri primi distinti e $k_i \geq 0, m_i \geq 0$ e $l_i \geq 0$ per ogni $i = 1, 2, \dots, s$. Prima di tutto osserviamo che per il corollario 3.11, $c|a$ se e solo se $l_i \leq k_i$ per ogni $i = 1, 2, \dots, s$. In particolare, $c|a$ e $c|b$ se e solo se $l_i \leq k_i$ e $l_i \leq m_i$ per ogni $i = 1, 2, \dots, s$. In altre parole, se e solo se $l_i \leq \min\{k_i, m_i\}$ per tutti gli $i = 1, 2, \dots, s$. Per questo il massimo comun divisore c di a e b è determinato da $l_i = \min\{k_i, m_i\}$ per tutti gli $i = 1, 2, \dots, s$.

Analogamente si ragiona per vedere che il minimo comune multiplo c di a e b deve avere $l_i = \max\{k_i, m_i\}$ per ogni $i = 1, 2, \dots, s$, oppure si applichi la formula $m.c.m.(a, b) = \frac{ab}{(a,b)}$.

Possiamo ora rispondere alla domanda posta all'inizio del paragrafo sui numeri primi e cioè quanti numeri primi esistono.

Teorema 3.13. (Euclide) *Esistono infiniti numeri primi.*

DIMOSTRAZIONE. Supponiamo che $p_1, p_2, \dots, p_n$ siano tutti i numeri primi e consideriamo il numero $N = p_1 p_2 \dots p_n + 1$. Poiché $p_1, p_2, \dots, p_n$ non dividono N (perché?), N deve essere primo e quindi coincide con uno dei $p_1, p_2, \dots, p_n$, assurdo. □

Possiamo addirittura "specializzare" la forma dei numeri primi, chiedendo per esempio quanti primi di un certo tipo esistono, come nell'esercizio 3.6.

3.5 Congruenze in $\mathbb{Z}$

Sia $m > 1$ un intero. Introduciamo nell'insieme $\mathbb{Z}$ la relazione binaria $a \equiv_m b$ detta *congruenza modulo* m. Diremo, per definizione, che *a è congruo a b modulo m* se m divide la differenza $a - b$. Verifichiamo innanzitutto che $\equiv_m$ è una relazione di equivalenza su $\mathbb{Z}$.

$a \equiv_m a$ per ogni $a \in \mathbb{Z}$ poiché m divide $0 = a - a$;
se $a \equiv_m b$, allora anche $b \equiv_m a$ per ogni coppia $a, b \in \mathbb{Z}$, poiché

$$m|(a-b) \quad \Longrightarrow \quad m|(b-a) = -(a-b);$$

se $a \equiv_m b$ e $b \equiv_m c$, allora anche $a \equiv_m c$, poiché

$$m|(a-b) \quad \text{e} \quad m|(b-c) \quad \Longrightarrow \quad m|(a-c) = (a-b) + (b-c).$$

Vediamo ora quali m sono rilevanti. Per $m = 0$ la relazione $a \equiv_0 b$ non si può introdurre come $m|(a - b)$, ma si potrebbe usare la conseguenza, cioè che $a - b$ è multiplo di m che ha senso anche quando $m = 0$. In tal senso

$$a \equiv_0 b \quad \text{se e solo se} \quad a = b,$$

quindi la congruenza $\equiv_0$ coincide con la solita uguaglianza "=". Per $m = \pm 1$ abbiamo $a \equiv_m b$ per ogni coppia a, b. Pertanto $\equiv_m$ ha una sola classe di equivalenza. Per finire, notiamo che $m|a - b$ se e solo se $-m|a - b$, quindi le relazioni $\equiv_m$ e $\equiv_{-m}$ coincidono. Per questi motivi in seguito considereremo solo $m > 1$.

Denotiamo con $[a]_m$ la classe di equivalenza di a, in altre parole

$$[a]_m = \{x \in \mathbb{Z} : \text{ esiste } y \in \mathbb{Z} \text{ con } x = a + my\} =$$
$$= \{\dots, a - m, a, a + m, a + 2m, \dots\}$$

cioè $[a]_m$ è la progressione aritmetica bilaterale di ragione m e punto iniziale a.

Si noti che la classe $[a]_m$ è *infinita*, mentre ci sono solo un numero finito di classi di equivalenza. Infatti questo segue subito dal seguente facile lemma.

Lemma 3.14. *Sia r il resto di a modulo m, cioè $a = qm + r$, con $0 \leq r < m$. Allora $a \equiv_m r$.*

Definizione 3.15. Sia $\mathbb{Z}_m = \mathbb{Z}/\equiv_m$ l'insieme quoziente rispetto a questa relazione di equivalenza. Chiamiamo $\mathbb{Z}_m$ l'*insieme delle classi resto modulo m*.

L'insieme $\mathbb{Z}_m$ viene tavolta denotato con $\mathbb{Z}/m\mathbb{Z}$, come chiarito nell'esempio 6.2.

Osservazione 3.16. Osserviamo che l'insieme

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

presenta tutte le classi di equivalenza modulo m e queste classi sono a due a due distinte, perché $k \not\equiv_m r$ quando $0 \leq k < m$, $0 \leq r < m$ e $k \neq r$.

Se $n|m$, allora $a \equiv_m b$ implica $a \equiv_n b$. Se $(n, m) = 1$, allora $a \equiv_{mn} b$ se e solo se $a \equiv_m b$ a $a \equiv_n b$. Infatti

$$m|(a-b) \quad \text{e} \quad n|(a-b) \quad \Longleftrightarrow \quad mn|(a-b)$$

per il corollario 3.11, poiché m e n sono coprimi.

Le seguenti proprietà delle congruenze sono collegate alle operazioni algebriche in $\mathbb{Z}$.

Lemma 3.17. *(a) Se $a \equiv_m a'$ e $b \equiv_m b'$, allora anche*

$$a + b \equiv_m a' + b' \quad e \quad ab \equiv_m a'b'.$$

(b) Se $ac \equiv_m bc$ e $(c, m) = 1$, allora anche

$$a \equiv_m b.$$

DIMOSTRAZIONE. (a) Si ha $m|(a - a')$ e $m|(b - b')$. Allora (d_1) del lemma 3.4 permette di concludere che

$$m|((a-a') + (b-b')) = (a+b) - (a'-b'),$$

quindi

$$a + b \equiv_m a' + b'.$$

Per quanto riguarda il prodotto presentiamo la differenza $ab - a'b'$ come

$$ab - ab' + ab' - a'b' = a(b-b') + b'(a-a').$$

Di nuovo il punto (d_1) del lemma 3.4 permette di concludere che

$$m|(a(b-b') + b'(a-a')) = ab - a'b'.$$

Quindi $ab \equiv_m a'b'$.

(b) Dai fatti che m divide $ac - bc = (a-b)c$ ed $(m, c) = 1$, segue che m divide $a - b$ per il lemma 3.8. □

Usando le classi di equivalenza possiamo scrivere (a) del lemma precedente anche nel modo seguente:

$$(a^*) \quad [a]_m = [a']_m \text{ e } [b]_m = [b']_m, \implies [a+b]_m = [a'+b']_m \text{ e } [ab]_m = [a'b']_m.$$

La proprietà (a*) permette di introdurre in $\mathbb{Z}_m$ due operazioni algebriche:

$$[a]_m + [b]_m = [a+b]_m \quad \text{e} \quad [a]_m[b]_m = [ab]_m.$$

Infatti (a*) garantisce che la somma $[a+b]_m$ dipende solamente dalle classi $[a]_m$ e $[b]_m$ e non dai particolari rappresentanti a, b.

3.6 Equazioni congruenziali ed equazioni diofantee

Consideriamo equazioni congruenziali di primo grado ad una variabile; cioè, dati $m > 1$, a e b numeri interi fissati con $a \neq 0$, cerchiamo le soluzioni $x \in \mathbb{Z}$ della congruenza

$$ax \equiv_m b. \tag{4}$$

Se x_0 è una soluzione di (4), lo sono anche tutti gli $x \equiv_m x_0$.

Teorema 3.18. *Siano $m > 1$, a e b numeri interi fissati con $a \neq 0$ e $d = (a, m)$. Allora l'equazione congruenziale (4) ha soluzione se e solo se d divide b. Se x_0 è una di tali soluzioni, tutte le soluzioni di (4) sono della forma $x_0 + nm_1$, al variare di $n \in \mathbb{Z}$ e con $m = m_1 d$.*

DIMOSTRAZIONE. Se (4) vale per x, allora m divide la differenza $ax - b$. Quindi d divide la differenza $ax - b$ e anche a. Allora d divide b.

Supponiamo che d divida b e dunque $b = db_1$ per qualche $b_1 \in \mathbb{Z}$. Si ha $a = a_1 d$ e $m = m_1 d$, con $a_1, m_1 \in \mathbb{Z}$ e $(a_1, m_1) = 1$. Inoltre si trovano numeri interi u, v tali che $d = au + mv$. Allora

$$b = db_1 = (au + mv)b_1 = a(ub_1) + mvb_1 \equiv_m a(ub_1).$$

Pertanto $x_0 = ub_1$ è una soluzione di (4). Verifichiamo ora che gli elementi del tipo $x_0 + nm_1$, al variare di $n \in \mathbb{Z}$, sono tutte soluzioni di (4). Infatti

$$a\,(x_0 + nm_1) = ax_0 + nam_1 \equiv_m b + nma_1 \equiv_m b.$$

D'altra parte, se x_1 è una soluzione di (4), allora $ax_1 \equiv_m ax_0$ e di conseguenza m divide $a(x_1 - x_0)$. Pertanto $a(x_1 - x_0) = km$ per qualche $k \in \mathbb{Z}$. Quindi, dividendo per d, $a_1(x_1 - x_0) = km_1$. Ora $(a_1, m_1) = 1$ implica $a_1|k$. Se $k = na_1$, si ha $x_1 = x_0 + nm_1$. □

Applichiamo il teorema 3.18 ad un caso concreto.

Esempio 3.19. Risolvere l'equazione congruenziale $143x \equiv_{57} 17$. Dividendo 143 per 57 troviamo $143 = 2 \cdot 57 + 29$, poi $57 = 29 + 28$ e $29 = 28 + 1$. Di qui $1 = 29 - 28 = 29 - (57 - 29) = 2 \cdot 29 - 57 = 2 \cdot (143 - 2 \cdot 57) - 57 = 2 \cdot 143 - 5 \cdot 57$. Quindi $x \equiv_{57} 2 \cdot 17 = 34$.

Un modo più veloce di lavorare è di sostituire subito 143 con il suo resto 29 modulo 57, cioè lavorare in partenza con l'equazione congruenziale $29x \equiv_{57} 17$. Ora con $29 \equiv_{57} -28$ e $17 \equiv_{57} -40$ si trova l'equazione congruenziale $-28x \equiv_{57} -40$. Poiché 4 e 57 sono coprimi possiamo cancellare 4 e si trova $-7x \equiv_{57} -10$ e di conseguenza

$$7x \equiv_{57} 10. \tag{5}$$

Poiché $57 = 8 \cdot 7 + 1$, abbiamo $8 \cdot 7 \equiv_{57} -1$. Quindi moltiplicando (5) per 8 si trova $8 \cdot 7x \equiv_{57} 80$ e pertanto $-x \equiv_{57} 23$ e $x \equiv_{57} -23 \equiv_{57} 34$.

Esempio 3.20. Trovare il resto del numero 341^{17} modulo 72.

$$341^{17} \equiv_{72} (-19)^{17} \equiv_{72} -(19)^{16} \cdot 19 \equiv_{72} -((19)^2)^8 \cdot 19 \equiv_{72} -(1)^8 \cdot 19 \equiv_{72} 53.$$

Affrontiamo ora le equazioni diofantee. Ogni terna a, b, c di numeri interi con $a \neq 0, b \neq 0$ determina una *equazione diofantea* di primo grado con due variabili

$$ax + by = c. \tag{6}$$

Cercheremo soluzioni x, y di (6) che siano numeri interi. Per ogni intero $m > 1$ consideriamo anche la congruenza

$$ax + by \equiv_m c \tag{7}$$

associata a (6). Ogni soluzione x, y di (6) è anche una soluzione di (7). Questo si estende in modo ovvio anche per equazioni diofantee di $n > 2$ variabili del tipo

$$\sum_{k=1}^{n} a_k x_k = c, \tag{8}$$

dove $c, a_1, a_2, \dots, a_n \in \mathbb{N}$ e la relative congruenza

$$\sum_{k=1}^{n} a_k x_k \equiv_m c, \tag{9}$$

cioè ogni soluzione $x_1, x_2, \dots, x_n$ di (8) è anche una soluzione di (9). Vediamo nel teorema 3.22 che questo risultato si può invertire nel seguente senso debole: se (9) ha soluzioni per ogni intero $m > 1$ allora anche (8) ha soluzioni.

Definiamo per induzione il massimo comun divisore di n numeri interi.

Definizione 3.21. Dati n numeri interi $m_1, \dots, m_n$, si definisce induttivamente il loro massimo comun divisore positivo, partendo dalla definizione nota nel caso $n = 2$ e definendo per $n \geq 3$, $(m_1, \dots, m_n) = ((m_1, \dots, m_{n-1}), m_n)$.

Si prova facilmente che $d = (m_1, \dots, m_n)$ divide m_i per ogni $i = 1, \dots, n$ e se m è un divisore comune degli m_i, $i = 1, \dots, n$, si ha che m divide d. Segue immediatamente dal teorema 3.7 che esistono $u_1, u_2, \dots, u_n \in \mathbb{Z}$ tali che $d = \sum_{k=1}^{n} a_k u_k$.

Analogamente si definisce il $m.c.m.(m_1, \dots, m_n)$.

Teorema 3.22. *Sia $n \in \mathbb{N}$ e siano $a_1, a_2, \dots, a_n$ e c numeri interi non nulli. Allora le seguenti condizioni sono equivalenti:*

(a) l'equazione diofantea (8) ha soluzioni;
(b) per ogni intero $m > 1$ la congruenza associata (9) ha soluzioni;
(c) il massimo comun divisore $(a_1, \dots, a_n)$ divide c.

DIMOSTRAZIONE. Come già detto sopra, (a) implica (b).

Supponiamo che, per ogni intero $m > 1$, la congruenza associata (9) abbia soluzioni. Se $a_n = \pm 1$, il massimo comun divisore d di $a_1, \ldots, a_{n-1}$ e a_n essendo uguale a 1 divide c. Quindi in questo caso (b) implica (c). Per dimostrarlo nel caso generale supponiamo ora $a_n \neq \pm 1$. Poniamo $m = |a_n| > 1$ e sia $d = (a_1, \ldots, a_{n-1}, m)$. Allora (9) diventa $\sum_{k=1}^{n-1} a_k x_k \equiv_m c$, e per ipotesi, (9) ammette soluzioni. Non è difficile vedere, ragionando come nella prima parte della dimostrazione del teorema 3.18, che questo implica che d divide c.

Infine, se d divide c, avremo $c = dc_1$ per qualche $c_1 \in \mathbb{Z}$. Come abbiamo notato sopra, esistono $u_1, u_2, \ldots, u_n \in \mathbb{Z}$ tali che $d = \sum_{k=1}^{n} a_k u_k$. Allora

$$x_1 = c_1 u_1, \quad \ldots, \quad x_{n-1} = c_1 u_{n-1}, \quad x_n = c_1 u_n$$

è una soluzione di (8). □

Esempio 3.23. Dimostrare che esiste un intero n_0, tale che per ogni $n \geq n_0$ l'equazione diofantea $3x + 8y = n$ ha almeno una soluzione $(x, y) \in \mathbb{N}^2$. Osserviamo che se $(x, y) \in \mathbb{N}^2$, si ha $n \geq 0$.

Se $n \equiv_3 0$, cioè $n = 3k$ per qualche $k \in \mathbb{N}$, si ha la soluzione $(k, 0)$.

Se $n \equiv_3 1$, allora $3x + 8y = 3k + 1$ per qualche $k \in \mathbb{N}$. L'equazione $8y \equiv_3 1$ ha soluzione per il teorema 3.18, e se cerchiamo una soluzione positiva, tale soluzione è del tipo $y = 2 + 3l$, per qualche $l \in \mathbb{N}$. Allora se $3x = 3(k - 8l - 5)$ ha una soluzione positiva, si ha $k \geq 5$.

Se $n \equiv_3 2$, allora $3x + 8y = 3k + 2$ per qualche $k \in \mathbb{N}$. L'equazione $8y \equiv_3 2$ ha soluzione per il teorema 3.18, e se cerchiamo una soluzione positiva, tale soluzione è del tipo $y = 1 + 3l$, per qualche $l \in \mathbb{N}$. Allora se $3x = 3(k - 8l - 2)$ ha una soluzione positiva, si ha $k \geq 2$.

Pertanto basta scegliere $n_0 \geq 14$.

Vediamo come possiamo utilizzare il teorema 3.22 e i risultati sulle equazioni congruenziali per risolvere equazioni diofantee anche non lineari.

Esempio 3.24. Dimostriamo che l'equazione diofantea $x^2 - 7y^2 = 14$ non ha soluzione intera. Osserviamo che 7 deve dividere x, pertanto 7 deve dividere $2 + y^2$. Si deve trovare un numero intero y tale che $y^2 \equiv_7 -2$. Ma un tale y non esiste, perché solo 1, 4 e 2 sono quadrati modulo 7. Pertanto non ci sono soluzioni intere.

Esempio 3.25. Dimostriamo che l'equazione diofantea $x^3 + 15y^3 = 24$ non ha soluzioni intere. Osserviamo che per ogni $x \in \mathbb{Z}$, si ha $x^3 \equiv_7 0, 1$, o -1, da cui $x^3 + 15y^3 \equiv_7 x^3 + y^3 \not\equiv_7 3 \equiv_7 24$ per ogni $y \in \mathbb{Z}$. Pertanto non ci sono soluzioni intere.

Vediamo ora un esempio di un *sistema di equazioni congruenziali*.

Esempio 3.26. Si trovi il minimo numero naturale n per cui risulti simultaneamente

$$\begin{cases} n \equiv_7 2 \\ n \equiv_6 1 \\ n \equiv_5 0. \end{cases}$$

Dalla prima congruenza ricaviamo $n = 2 + 7\lambda$ per qualche $\lambda \in \mathbb{Z}$, che sostituita nella seconda implica $n = 2 + 7\lambda \equiv_6 1$. Pertanto $7\lambda \equiv_6 1 - 2$, cioè $\lambda \equiv_6 5$ e quindi esiste $k \in \mathbb{Z}$ tale che $\lambda = 5+6k$. Sostituendo si ottiene $n = 2+(5+6k)7 = 37+42k$ che sostituita nell'ultima dà

$$37 + 42k \equiv_5 0 \Rightarrow 2 + 2k \equiv_5 0 \Rightarrow k \equiv_5 -1 \equiv_5 4,$$

usando il lemma 3.17 in quanto (2,5)=1.

Allora esiste $h \in \mathbb{Z}$ tale che $k = 4 + 5h$ e così

$$n = 37 + 42k = 37 + 42(4 + 5h) = 205 + 210h.$$

Le soluzioni intere sono quindi del tipo $n = -5 + 210m$ e dunque si avrà $n = 205$.

Osserviamo che nell'esempio 3.26, il massimo comune divisore di ogni coppia tra i numeri $7, 6, 5$ è 1. Nel seguente *teorema cinese del resto* dimostreremo che questa è proprio la condizione necessaria e sufficiente perché ogni sistema di equazioni congruenziali di quel tipo ammetta delle soluzioni.

Teorema 3.27. (Teorema cinese del resto) *Siano $m_1, \ldots, m_n \in \mathbb{Z}$ maggiori di 1. Si consideri il sistema di congruenze*

$$\begin{cases} x \equiv_{m_1} a_1 \\ \ldots \\ x \equiv_{m_i} a_i \\ \ldots \\ x \equiv_{m_n} a_n. \end{cases} \tag{10}$$

Allora il sistema (10) *ammette una soluzione per ogni n-upla $a_1, \ldots, a_n \in \mathbb{Z}$ se e solo se $(m_i, m_j) = 1$ per ogni $i, j = 1, \ldots, n$, $i \neq j$.*

In tal caso, se x_0 è una soluzione, l'insieme di tutte le soluzioni in $\mathbb{Z}$ è

$$S = \{x_0 + mz : m = m_1 \ldots m_n,\ z \in \mathbb{Z}\}.$$

DIMOSTRAZIONE. Supponiamo che il sistema (10) abbia una soluzione per ogni n-upla $a_1, \ldots, a_n \in \mathbb{Z}$. Siano $i, j \in \{1, \ldots, n\}$ con $i \neq j$ e per ogni $l = 1, \ldots, n$ $l \neq j$ poniamo $a_l = 0$ e $a_j = 1$. Allora esiste una soluzione x_0 tale che $x_0 \equiv_{m_i} 0$ e $x_0 \equiv_{m_j} 1$. Pertanto $x_0 = m_i u = m_j v + 1$ per qualche $u, v \in \mathbb{Z}$, da cui segue che $(m_i, m_j) = 1$.

Supponiamo viceversa che $(m_i, m_j) = 1$ per ogni $i, j = 1, \ldots, n$, $i \neq j$. Dimostriamo per induzione su n che esiste una soluzione di (10). Sia $n = 2$ e consideriamo il sistema

$$\begin{cases} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2. \end{cases}$$

Una soluzione alla prima congruenza è del tipo $x = a_1 + m_1 s$ per qualche $s \in \mathbb{Z}$. Sostituiamo nella seconda congruenza, e abbiamo $m_1 s \equiv_{m_2} a_2 - a_1$ che per il teorema 3.18 ha soluzione per ogni coppia (a_1, a_2) se e solo se $(m_1, m_2) = 1$. Sia ora x_0 una soluzione, allora $x_0 + m_1 m_2 z$, $z \in \mathbb{Z}$ è ancora una soluzione. Viceversa, se a è un'altra soluzione del sistema, si ha $a - x_0 \equiv_{m_i} 0$ per $i = 1, 2$ da cui $a = x_0 + m_1 m_2 z$, in quanto $(m_1, m_2) = 1$.

Sia ora $n \geq 3$. Consideriamo il sistema

$$\begin{cases} x \equiv_{m_1} a_1 \\ \dots \\ x \equiv_{m_i} a_i \\ \dots \\ x \equiv_{m_{n-1}} a_{n-1}. \end{cases} \tag{11}$$

Per ipotesi induttiva, tale sistema ha soluzione per ogni $(n-1)$-upla $a_1, \dots, a_{n-1} \in \mathbb{Z}$ se e solo se $(m_i, m_j) = 1$, per ogni $i, j = 1, \dots, n-1$, $i \neq j$. Sia b una soluzione del sistema (11), e sia $l = m.c.m.(m_1, \dots, m_{n-1}) = m_1 m_2 \dots m_{n-1}$. Consideriamo il sistema

$$x \equiv_l b; \qquad x \equiv_{m_n} a_n. \tag{12}$$

Per il caso $n = 2$, tale sistema ha soluzione se e solo se $(l, m_n) = 1$, che è equivalente a $(m_i, m_n) = 1$, per ogni $i = 1, \dots, n-1$. Se x_0 è una soluzione di (12), allora per ogni $i = 1, \dots, n-1$ si ha $x_0 \equiv_{m_i} b \equiv_{m_i} a_i$. Pertanto x_0 è una soluzione anche di (10). Infine, per il caso $n = 2$, abbiamo che l'insieme delle soluzioni risulta essere $S = \{x_0 + l m_n z : z \in \mathbb{Z}\} = \{x_0 + m_1 \dots m_{n-1} m_n z : z \in \mathbb{Z}\}$. □

3.7 Alcuni criteri di divisibilità

In questo paragrafo dimostriamo alcuni criteri di divisibilità e introduciamo alcuni sistemi di numerazione.

Teorema 3.28. *Sia $m > 1$ intero. Per ogni numero intero positivo a esistono dei numeri naturali $a_0, a_1, a_2, a_3, \dots, a_k$ tali che $0 \leq a_i < m$ per $i = 0, 1, \dots, k$ e*

$$a = a_0 + a_1 m + a_2 m^2 + a_3 m^3 + \ldots + a_i m^i + \ldots + a_k m^k. \tag{13}$$

DIMOSTRAZIONE. Possiamo trovare il resto a_0 nella divisione di a per m,

$$a = q_1 m + a_0.$$

Possiamo trovare il resto a_1 di q_1 modulo m per avere $q_1 = q_2 m + a_1$ e di conseguenza $a = q_2 m^2 + a_1 m + a_0$. Proseguendo in questo modo otteniamo una successione

di resti $a_0, a_1, a_2, a_3, \ldots$ e di dividendi $q_1 > q_2 > \ldots$ tali che $q_i = q_{i+1}m + a_i$ per ogni $i = 1, 2, \ldots$ e quindi

$$a = a_0 + a_1 m + a_2 m^2 + \ldots + a_i m^i + \ldots + a_k m^k + q_{k+1} m^{k+1}.$$

Poiché la successione q_i decresce strettamente, avremo $q_{k+1} = 0$ per un certo k, per il quale si avrà (13). □

I numeri $a_0, a_1, a_2, a_3, \ldots a_k$ si chiamano *cifre* di a in base m e si scrive

$$a = \overline{a_k \ldots a_1 a_0}_{(m)}.$$

In particolare, con $m = 10$ si hanno le cifre decimali e si scrive brevemente

$$a = \overline{a_k \ldots a_1 a_0} \quad \text{invece di} \quad a = \overline{a_k \ldots a_1 a_0}_{(10)}.$$

Particolare importanza ha recentemente assunto il sistema di numerazione binaria, cioè la scrittura dei numeri in base 2, in quanto l'uso delle sole cifre 0, 1 permette di tradurre ogni numero naturale in una stringa di 0 e 1, che trova molte applicazioni nell'informatica.

Esempio 3.29. Non è difficile verificare che $71 = \overline{1000111}_{(2)}$.

Dimostriamo nella seguente proposizione l'usuale "prova del 9".

Proposizione 3.30. *Siano $a_0, a_1, a_2, a_3, \ldots, a_k$ le cifre decimali di a e sia*

$$S = a_0 + a_1 + a_2 + \ldots + a_k.$$

Allora $a \equiv_9 S$. In particolare:

(a) a è divisibile per 3 se e solo se S è divisibile per 3;
(b) a è divisibile per 9 se e solo se S è divisibile per 9.

DIMOSTRAZIONE. Si ha $10 \equiv_9 1$, quindi $10^i \equiv_9 1$ per ogni $i = 1, 2, \ldots, k$. Moltiplicando per a_i si ricava $a_i 10^i \equiv_9 a_i$ per ogni $i = 1, 2, \ldots, k$. Sommando si ricava $a = a_0 + a_1 10 + a_2 10^2 + \ldots + a_k 10^k \equiv_9 S$. Ora (a) e (b) seguono immediatamente da $a \equiv_9 S$. □

Proposizione 3.31. *Siano $a_0, a_1, a_2, a_3, \ldots, a_k$ le cifre decimali di a e sia*

$$S = a_0 - a_1 + a_2 + \ldots + (-1)^k a_k = \sum_{i=0}^{k} (-1)^i a_i.$$

Allora $a \equiv_{11} S$. In particolare a è divisibile per 11 se e solo se S è divisibile per 11.

DIMOSTRAZIONE. Poiché $10 \equiv_{11} -1$, si ha $10^i \equiv_{11} (-1)^i$ per ogni $i = 1, 2, \ldots, k$. Moltiplicando per a_i si ricava $a_i 10^i \equiv_{11} (-1)^i a_i$ per ogni $i = 1, 2, \ldots, k$. Sommando si ricava $a = a_0 - a_1 10 + a_2 10^2 - \ldots + (-1)^k a_k 10^k \equiv_{11} S$. La seconda affermazione segue dalla prima. □

Proposizione 3.32. *Siano $a_0, a_1, a_2, a_3, \ldots, a_n$ le cifre decimali di a, sia $m = [n/2]$ e sia S definito nel modo seguente:*

(a)

$$S = \overline{a_1 a_0} - \overline{a_3 a_4} + \ldots + (-1)^k \overline{a_{2k+1} a_{2k}} + \ldots + (-1)^m \overline{a_{2m+1} a_{2m}} =$$

$$= \sum_{k=0}^{m} (-1)^k a_{2k+1} a_{2k},$$

se $n = 2m + 1$ è dispari; e

(b)

$$S = \overline{a_1 a_0} - \overline{a_3 a_4} + \ldots + (-1)^k \overline{a_{2k+1} a_{2k}} + \ldots +$$

$$+ (-1)^{m-1} \overline{a_{2m-1} a_{2m-2}} + (-1)^m a_{2m} =$$

$$= \left(\sum_{k=0}^{m-1} (-1)^k \overline{a_{2k+1} a_{2k}} \right) + (-1)^m a_{2m},$$

se $n = 2m$ è pari.

Allora $a \equiv_{101} S$. In particolare a è divisibile per 101 se e solo se S è divisibile per 101.

DIMOSTRAZIONE. Si ha $100 \equiv_{101} -1$, quindi $100^i \equiv_{101} (-1)^i$ per ogni $i = 1, 2, \ldots, k$. Pertanto nel caso (a) si ha

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \ldots + a_i \cdot 10^i + \ldots + a_n \cdot 10^n \equiv_{101}$$

$$\equiv_{101} a_0 + a_1 \cdot 10 - a_2 - a_3 \cdot 10 + a_4 + a_5 \cdot 10 - \ldots$$

$$\ldots + (-1)^k (a_{2k} + a_{2k+1} \cdot 10) + \ldots + (-1)^m (a_{2m} + a_{2m+1} \cdot 10).$$

Il caso (b) è analogo.
La seconda affermazione segue dalla prima. □

Applicando questo criterio si vede immediatamente che 101 dvide 786386, in quanto $86 - 63 + 78 = 101$.

3.8 Il teorema di Fermat

Il seguente importante teorema è dovuto a Fermat. Vedremo più avanti come questo sia un caso particolare di un teorema più generale dovuto ad Eulero.

Teorema 3.33. (Piccolo teorema di Fermat) *Sia p un numero primo. Allora*

$$a^p \equiv_p a \quad \text{per ogni numero intero} \quad a.$$

DIMOSTRAZIONE. Supponiamo dapprima $a \geq 0$ e usiamo l'induzione. Se $a = 0$ è ovvio. Supponiamo l'asserto vero per qualche $a > 0$ e lo vogliamo dimostrare per $a + 1$. Per l'esercizio 3.56 (b), sappiamo che $(a+1)^p \equiv a^p + 1$, da cui, usando l'ipotesi induttiva che garantisce $a^p \equiv_p a$, si ha $(a+1)^p \equiv_p a + 1$. Supponiamo ora $a < 0$. Allora $0 \equiv_p 0^p \equiv_p (a + (-a))^p \equiv_p a^p + (-a)^p \equiv_p a^p - a$, ancora per l'esercizio 3.56 e per il fatto che $-a > 0$ e quindi l'asserto è vero per $-a$. □

Lemma 3.34. *Siano p un numero primo e a un intero coprimo con p. Per il teorema di Fermat esiste un numero naturale $n > 0$ con la proprietà $a^n \equiv_p 1$. Sia k il più piccolo di tali n, allora k ha le seguenti proprietà*

(a) $a^{qk} \equiv_p 1$ per ogni intero $q \geq 0$;
(b) se $a^n \equiv_p 1$ per un intero $n \geq 0$, allora k divide n.

DIMOSTRAZIONE. (a) È sufficiente elevare alla q la congruenza $a^k \equiv_p 1$. Per dimostrare (b), si divida n per k con resto r, cioè $n = qk + r$, con $0 \leq r < k$. Ora per (a) avremo $1 \equiv_p a^n = a^{qk+r} = a^{qk} \cdot a^r \equiv_p 1 \cdot a^r$. Di conseguenza $a^r \equiv_p 1$. Per la scelta di k si ha $r = 0$, cioè k divide n. □

Nel seguito denoteremo con $o_p(a)$ il numero k definito nel lemma 3.34.

Lemma 3.35. *Sia p un numero primo e a un intero coprimo con p. Allora:*

(a) $o_p(a)$ divide $p - 1$;
(b) se $p > 2$, allora $a^{\frac{p-1}{2}} \equiv_p \pm 1$.

DIMOSTRAZIONE. (a) Si applichi il piccolo teorema di Fermat 3.33 e (b) del lemma 3.34.

(b) Poiché p è primo e divide $a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$, concludiamo che p divide uno dei due fattori. □

Notiamo che $a^{\frac{p-1}{2}} \equiv_p -1$ non implica $o_p(a) = p - 1$.

3.9 Funzione di Eulero e teorema di Eulero

Ci proponiamo di contare il numero di interi positivi coprimi con un numero naturale n e minori di n.

Definizione 3.36. Poniamo $\varphi(1) = 1$ e per un numero naturale $n > 1$ poniamo $\varphi(n)$ uguale al numero dei numeri naturali k coprimi con n e soddisfacenti $1 \leq k < n$. La funzione $\varphi(n)$ è nota come *funzione di Eulero* o *funzione totiente*.

Vediamo una prima utilissima proprietà della funzione di Eulero.

Lemma 3.37. *Siano m ed n due numeri naturali coprimi tra loro. Allora*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

DIMOSTRAZIONE. Siano

$$U = \{u_1, \ldots, u_{\varphi(n)}\}, \quad V = \{v_1, \ldots, v_{\varphi(m)}\} \quad \text{e} \quad W = \{w_1, \ldots, w_{\varphi(nm)}\}$$

gli insiemi dei numeri interi coprimi con n, m ed nm e minori di n, m, nm, rispettivamente. Poiché $|U \times V| = \varphi(n)\varphi(m)$ e $|W| = \varphi(nm)$, per dimostrare il lemma sarà sufficiente costruire una biezione tra $U \times V$ e W. Sia dunque $(u, v) \in U \times V$. Per il teorema cinese del resto 3.27, il sistema di equazioni congruenziali $x \equiv_n u$, $x \equiv_m v$ ammette un'unica soluzione w con l'ulteriore condizione $1 \leq w \leq mn$. Osserviamo che $w \equiv_n u$ e $w \equiv_m v$ implicano che w è coprimo sia con m che con n, in quanto tali sono u e v. Allora $w \in W$ e quindi la posizione $f(u, v) = w$ definisce un'applicazione $f : U \times V \to W$. Verifichiamo che f è iniettiva: infatti se $f(u, v) = w = f(u', v')$, si ha $u \equiv_n w \equiv_n u'$, e poiché $1 \leq u, u' < m$, si ha $u = u'$; analogamente $v = v'$. Infine consideriamo $w \in W$ e sia u il resto della divisione euclidea di w per n. Allora $w \equiv_n u$, $0 \leq u < n$ e poiché w è coprimo con mn, u è coprimo con n. Allora $u \in U$, analogamente esiste $v \in V$ tale che $w \equiv_m v$. Concludiamo che $f(u, v) = w$. □

Lemma 3.38. *Sia p un numero primo e sia $n > 0$ un numero naturale. Allora $\varphi(p^n) = p^n - p^{n-1}$.*

DIMOSTRAZIONE. Basta contare quanti sono i numeri $k \leq p^n$ che *non sono* coprimi con p^n. Chiaramente k non è coprimo con p^n se e solo se k è divisibile per p. Quindi $k = pk_1$ per qualche $k_1 \in \mathbb{Z}$. Ora $k \leq p^n$ implica $k_1 \leq p^{n-1}$. Ci sono p^{k-1} numeri k tra 1 e p^k che non sono coprimi con p^n, da cui $\varphi(p^n) = p^n - p^{n-1}$. □

Gli ultimi due lemmi permettono di dimostrare il seguente teorema.

Teorema 3.39. *Se $m = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$ è la decomposizione di m in prodotto di potenze di numeri primi tra loro diversi, allora*

$$\varphi(m) = (p_1^{n_1} - p^{n_1 - 1})(p_2^{n_2} - p_2^{n_2 - 1}) \cdot \ldots \cdot (p_s^{n_s} - p_s^{n_s - 1}) =$$
$$= m\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_s}\right).$$

Come preannunciato, il seguente fatto (noto come teorema di Eulero) è una generalizzazione del piccolo teorema di Fermat.

Teorema 3.40. (Teorema di Eulero) *Se $a > 1$ e $m > 1$ sono due numeri naturali coprimi, allora $a^{\varphi(m)} \equiv_m 1$.*

DIMOSTRAZIONE. Sia $R = \{1, \ldots, m-1\}$ l'insieme dei resti modulo m coprimi con m. Definiamo un'applicazione $\alpha : R \to R$ nel modo seguente. Per $k \in R$ dividiamo ak per m con resto. Si ricava così un resto r_k soddisfacente $ak = qm + r_k$, e quindi $0 \leq r_k < m$ e

$$ak \equiv_m r_k \text{ per } k = 1, 2, \ldots m - 1. \tag{14}$$

Poiché k ed a sono entrambi coprimi con m, m è coprimo con ak e concludiamo che $r_k \in R$. Pertanto possiamo definire $\alpha(k) := r_k \in R$. Se $r_k = r_i$ per $i, k \in R$ avremo da (14) $ak \equiv_m r_k = r_i \equiv_m ai$, e quindi $ak \equiv_m ai$. Poiché a è coprimo con m, lo possiamo cancellare. Quindi $k \equiv_m i$ e per la definizione di R, $k = i$. Abbiamo così verificato che α è un'applicazione iniettiva. Quindi l'immagine $\alpha(R)$ dovrà avere $\varphi(m)$ elementi come R stesso. Essendo $\alpha(R)$ anche un sottoinsieme di R, avremo $\alpha(R) = \{r_1, \ldots, r_{\varphi(m)}\} = R$. In particolare, il prodotto $r_1 \cdot \ldots \cdot r_{\varphi(m)}$ coincide con il prodotto Π di tutti i resti in R, cioè

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} = \Pi. \tag{15}$$

Moltiplicando le $\varphi(m)$ congruenze in (14) otteniamo $a^{\varphi(m)} \cdot \Pi \equiv_m r_1 \cdot \ldots \cdot r_{\varphi(m)}$. Ora (15) permette di sostituire $r_1 \cdot \ldots \cdot r_{\varphi(m)}$ con Π in questa congruenza e ottenere $a^{\varphi(m)} \cdot \Pi \equiv_m \Pi$. Essendo Π coprimo con m possiamo cancellare Π e ricavare $a^{\varphi(m)} \equiv_m 1$. □

Vediamo ora un altro modo per risolvere le equazioni congruenziali del tipo $ax \equiv_m b$, nel caso in cui $(a, m) = 1$. Si ha infatti, grazie al teorema di Eulero, che $a^{\varphi(m)} \equiv_m 1$, da cui si ricava $a(a^{\varphi(m)-1}b) \equiv_m b$, per cui una soluzione si ottiene immediatamente ponendo $x_0 = a^{\varphi(m)-1}b$. Se si vuole ottenere una soluzione dell'equazione congruenziale anche nel caso generale usando il teorema di Eulero, ci si può poi ridurre al caso appena visto "dividendo" l'equazione per $d = (a, m)$.

3.10 I numeri di Fermat e di Mersenne

In questa sezione introduciamo due celebri "generatori di numeri primi", i numeri di Fermat e i numeri di Mersenne, legati in modo del tutto naturale ai numeri primi e ai numeri perfetti ed amicabili.

I numeri $F_n = 2^{2^n} + 1$, per $n = 0, 1, 2, \ldots$ sono noti come *numeri di Fermat.*

Osserviamo subito che se vogliamo ottenere dei numeri primi aggiungendo 1 a potenze di 2, dobbiamo imporre all'esponente di essere esso stesso una potenza di 2, come si dimostra nell'esercizio 3.20.

Lemma 3.41. *(a) Se p è un divisore primo del numero di Fermat F_n, allora p è del tipo $2^{n+1}m + 1$.*
(b) I numeri di Fermat sono a due a due coprimi.

DIMOSTRAZIONE. (a) Si noti che $p|F_n$ implica $2^{2^n} \equiv_p -1$ e di conseguenza, elevando al quadrato, $2^{2^{n+1}} \equiv_p 1$. Quindi $o_p(2)$ divide 2^{n+1}. Ora, per il punto (a) del lemma 3.34, la prima congruenza dimostra che $o_p(2)$ non è un divisore di 2^n. Poiché tutti i divisori di 2^{n+1} sono del tipo 2^k, concludiamo che $o_p(2) = 2^{n+1}$. Per il teorema di Fermat $2^{p-1} \equiv_p 1$. Ora (b) del lemma 3.34 permette di concludere che 2^{n+1} divide $p - 1$. Dunque $p - 1 = 2^{n+1}m$ per qualche $m \in \mathbb{Z}$.

(b) Se p è un primo che divide F_n ed F_m, con $n > m$, allora $2^{2^{m+1}} \equiv_p 1$ come nel punto (a). Poiché $m + 1 \leq n$, 2^{2^n} è potenza di $2^{2^{m+1}}$ e quindi $2^{2^n} \equiv_p 1$. D'altra

parte, $p|F_n$ implica anche $2^{2^n} \equiv_p -1$, assurdo. Pertanto nessun numero primo p divide simultaneamente F_n ed F_m, quindi F_n e F_m sono coprimi. □

Il punto (b) del lemma precedente porta a una dimostrazione alternativa del fatto che esistono infiniti numeri primi.

Ci si può a questo punto chiedere quali di questi numeri di Fermat siano effettivamente dei primi. La risposta per i primi 5 numeri di Fermat è stata data da Eulero nel 1732. Si osservi che, a parte F_0, F_1, F_2, F_3 e F_4, non sono noti altri numeri di Fermat primi.

Proposizione 3.42. *F_0, F_1, F_2, F_3 e F_4 sono primi, mentre $F_5 = 641 \cdot 6700417$ non è primo.*

DIMOSTRAZIONE. Per $F_0 = 3$, $F_1 = 5$ e $F_2 = 17$ questo è ovvio. Segue dall'esercizio 3.21 che per verificare se F_n è primo basta vedere che F_n non ha divisori primi $p < F_{n-1} - 1$. Per $F_3 = 257$ notiamo che i divisori primi di F_3 con $p < 16 = F_2 - 1$ possono essere tra $2, 3, 5, 7, 11$ e 13. Secondo il lemma 3.41, i divisori primi di F_3 sono del tipo $16k + 1$ e quindi nessuno di questi primi divide F_3.

Per $F_4 = 2^{16} + 1$ notiamo che per il lemma 3.41 i divisori primi di F_4 sono del tipo $32k + 1$. Ma i numeri di questo tipo minori di $F_3 - 1 = 256$ sono 33, 65, 97, 129, 161, 193 e 225. Tra questi solo 97 e 193 sono primi. Che nessuno dei primi 97 e 193 divida F_4 segue dallo svolgimento dell'esercizio 3.17.

Per F_5 sappiamo dal lemma 3.41 che i divisori primi di F_5 sono del tipo $64k + 1$. Tra questi 65 e 129 non sono primi. Dal suggerimento all'esercizio 3.17 segue che né 193 né 257 dividono $F_5 = 2^{32} + 1$. Tra i numeri successivi in questa serie 321, 385 e 513 non sono primi, mentre 449 e 577 sono primi ma non dividono F_5. Per 641 si dimostra che divide F_5 osservando che da $641 = 2^4 + 5^4 = 2^7 \cdot 5 + 1$ seguono le congruenze $2^4 \equiv_{641} -5^4$ e $2^7 \cdot 5 \equiv_{641} -1$. Elevando l'ultima congruenza alla quarta e sostituendo 5^4 con -2^4 si ha

$$1 \equiv_{641} 2^{28} \cdot 5^4 \equiv_{641} -2^{28} \cdot 2^4 \equiv_{641} -2^{32},$$

cioè 641 divide F_5. □

I numeri del tipo $M_n = 2^n - 1$ sono noti come *numeri di Mersenne*, dato che Marin Mersenne (1588-1648) li studiò in modo sistematico nel suo trattato "Cogita physico-matematica". Tuttavia questi numeri erano noti anche prima per esempio ai Greci, come ricordiamo nel paragrafo 3.11 e al matematico italiano Pietro Antonio Cataldi (1548-1626) che provò che M_{17} e M_{19} sono primi.

Si può vedere che M_n è primo solo se n è primo (si veda l'esercizio 3.22), tuttavia M_{11} non è primo: si verifica che è divisibile per 23, elevando al quadrato la congruenza $2^6 \equiv_{23} -5$. Nel seguito si chiarisce perché si verifica con 23 il fatto che M_{11} non sia primo: è il più piccolo numero primo che ha resto 1 modulo 11.

Gran parte dei numeri di Mersenne sono composti. Tuttavia, per lungo tempo, i più grandi numeri primi noti sono stati i numeri primi di Mersenne. Questo è dovuto al seguente criterio scoperto da Lucas che fa uso dei numeri L_n, detti *numeri di Lucas*, definiti da $L_1 = 4$ e $L_n = L_{n-1}^2 - 2$ per $n > 1$.

Teorema 3.43. *Per $n > 2$, il numero M_n è primo se e solo se M_n divide il numero L_{n-1}.*

Non diamo la dimostrazione di questo teorema, ma facciamo alcune verifiche. Si vede facilmente che $M_3 = 7$ divide $L_2 = 14$,

$$M_5 = 31 \quad \text{divide} \quad L_4 = L_3^2 - 2 = 194^2 - 2 = 37634 :$$

infatti $194 \equiv_{31} 8$ e quindi $L_4 \equiv_{31} 8^2 - 2 = 62 \equiv_{31} 0$. Per $n = 7$ si ha $M_7 = 127$, mentre $L_5 = 1416317954 \equiv_{127} 42^2 - 2$, poiché

$$L_4 \equiv_{127} 67^2 - 2 \equiv_{127} 67 + 66 \cdot 67 - 2 = 65 + 33 \cdot 134 \equiv_{127}$$
$$\equiv_{127} 65 + 33 \cdot 7 = 65 + 231 \equiv_{127} 42.$$

Ora $L_5 \equiv_{127} 126 \cdot 14 - 2 \equiv_{127} -14 - 2 = -16$, quindi

$$L_6 \equiv_{127} 16^2 - 2 = 2 \cdot 8 \cdot 16 - 2 = 2(8 \cdot 16 - 1) = 2 \cdot 127 \equiv_{127} 0.$$

Lasciamo al lettore la verifica del fatto che M_{11} non divide L_{10}, non essendo M_{11} un numero primo. D'altra parte, M_{13} divide L_{12}, essendo M_{13} un numero primo, come si dimostra nell'esercizio 3.25.

Usando questo criterio Lucas provò nel 1875 che il numero M_{127} è primo e questo risultato rimase insuperato per 75 anni data la grandezza di

$$M_{127} = 2^{127} - 1 = 170141183460469231731687303715884105727.$$

Il più grande numero primo scoperto senza l'uso dei calcolatore nel 1951 fu il numero $\frac{2^{148}+1}{17}$, con 44 cifre, mentre M_{127} ne ha *solo* 39. Sempre nel 1951, con l'uso dei calcolatori, venne invece scoperto che il numero $180(M_{127})^2 + 1$ è primo. I numeri M_{23209} e M_{44497} sono primi ed erano i più grandi numeri primi noti verso l'inizio degli anni Ottanta del secolo scorso. Il più grande numero primo noto nel settembre 2006 è $M_{32582657}$ con 9808358 cifre.

L'importanza dei numeri primi di Mersenne diverrà più chiara nel paragrafo successivo.

3.11 Numeri perfetti e numeri amicabili

In questa sezione introduciamo i numeri perfetti ed amicabili, legati in modo del tutto naturale ai numeri primi. Sia n un numero intero positivo. Si denoti con $\sigma(n)$ la somma dei divisori positivi di n. Chiaramente la somma $\sigma(n) - n$ di tutti i divisori di *n minori* di n misura, in un certo senso, la quantità di divisori di n. I numeri n con pochi divisori, cioè $\sigma(n) - n < n$ si dicono *scarsi*, mentre quelli con molti divisori, cioè $\sigma(n) - n > n$ si dicono *abbondanti*. Per esempio 10 è scarso, tutti i numeri primi sono scarsi, mentre 12 e 60 sono abbondanti. Per questo motivo i matematici antichi, per esempio a Babilonia, preferivano i sistemi di numerazione a base 12 o 60. Da questo punto di vista si capisce perché la scelta del termine numero perfetto nella seguente definizione.

Definizione 3.44. Un numero naturale n dicesi *perfetto* se $\sigma(n) = 2n$.

I numeri perfetti erano ben noti nell'antica Grecia. Prima di descrivere tutti i numeri perfetti pari vedremo alcune utili proprietà della funzione σ.

Lemma 3.45. *(a) Se p è primo, allora* $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$;
(b) Se $n = n_1 n_2$ *con* $(n_1, n_2) = 1$, *allora* $\sigma(n) = \sigma(n_1)\sigma(n_2)$.
(c) Se $n = p_1^{k_1} \dots p_s^{k_s}$, *allora* $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_1^{k_s+1}-1}{p_s-1}$.

DIMOSTRAZIONE. (a) Tutti i divisori di p^k sono del tipo p^s per $0 \le s \le k$.

(b) Se d divide $n_1 n_2$, allora raccogliendo i primi che compaiono nella fattorizzazione di n_1 e quelli che appaiono nella fattorizzazione di n_2, troviamo una fattorizzazione $d = d_1 d_2$ con $d_1 | n_1$ e $d_2 | n_2$. Quindi

$$\sigma(n_1 n_2) = \sum_{d | n_1 n_2} d = \sum_{d_1 | n_1, d_2 | n_2} d_1 d_2 = \left(\sum_{d_1 | n_1} d_1\right)\left(\sum_{d_2 | n_2} d_2\right) = \sigma(n_1)\sigma(n_2).$$

(c) segue da (a) e (b). □

Il punto (a) del seguente teorema si trova nel famoso trattato di Euclide. Il punto (b) è stato dimostrato da Eulero.

Teorema 3.46. *(a) Sia* $p = 2^n - 1$ *un numero primo. Allora*

$$\frac{1}{2}p(p+1) = 2^{n-1}(2^n - 1) \text{ è perfetto.}$$

(b) Ogni numero perfetto pari è di questo tipo.

DIMOSTRAZIONE. (a) Se $2^n - 1$ è un numero primo, usando (a) e (b) del lemma 3.45 si ha

$$\sigma(2^{n-1}(2^n - 1)) = \sigma(2^{n-1})\sigma(2^n - 1) = (2^n - 1)2^n.$$

(b) Sia $n = 2^s n_1$ un numero perfetto, con n_1 dispari e $s \ge 1$. Allora l'ipotesi $\sigma(n) = 2n$ implica

$$(2^{s+1} - 1)\sigma(n_1) = 2^{s+1} n_1,$$

da cui $2^{s+1} - 1$ divide n_1. Sia $n_1 = (2^{s+1} - 1)k$. Quindi $\sigma(n_1) = 2^{s+1}k$. Dunque $k = 1$, perché altrimenti

$$\sigma(n_1) \ge n_1 + k + (2^{s+1} - 1) + 1 = 2^{s+1}k + 2^{s+1} > 2^{s+1}k.$$

Ora $\sigma(n_1) = n_1 + 1$ implica che $n_1 = 2^{s+1} - 1$ è primo. □

Il teorema dice in sostanza che i numeri perfetti pari sono del tipo $2^{n-1} M_n$, dove M_n è un primo di Mersenne. Non è ancora noto se esistono numeri perfetti dispari.

Nell'antichità conoscevano anche i cosiddetti numeri *amicabili*, cioè coppie di numeri naturali a e b, tali che ognuno sia uguale alla somma dei divisori propri dell'altro. In termini più precisi,

$$\sigma(a) - a = b \quad \text{e} \quad \sigma(b) - b = a.$$

Quindi $\sigma(a) = a + b = \sigma(b)$. La prima coppia di numeri amicabili proviene da Pitagora (575 a.C. - 490 a.C. circa): sono i numeri 220 e 284. Si racconta addirittura che, alla domanda "Che cos'è un amico?", il grande Pitagora abbia risposto: "Uno che sia l'altro 'Io', come 220 e 284".

Il seguente teorema del matematico arabo Thabit ibn Qurra (836–901) fornisce altre coppie di numeri amicabili.

Lemma 3.47. *Se i numeri* $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ *ed* $r = 9 \cdot 2^{2n-1} - 1$ *sono primi, allora i numeri* $A = 2^n \cdot p \cdot q$ *e* $B = 2^n \cdot r$ *sono amicabili.*

DIMOSTRAZIONE. La dimostrazione segue facilmente dal lemma 3.45. □

Con $n = 2$ troviamo la coppia 220 e 284 di Pitagora. Non è noto se Thabit conoscesse altri casi oltre a questo. Altre coppie si trovano con $n = 4$, $A = 17296$, $B = 18416$ scoperta da Fermat, ma nota molto prima anche a Ibn Al Banna del Marocco (1256-1321) e $n = 7$ scoperta da Cartesio, René Descartes (1596 -1650). Entrambi sono arrivati in modo autonomo al teorema di Thabit che nel frattempo era stato completamente dimenticato. Eulero scoprì 59 coppie di numeri amicabili. Il suo record è stato superato solo nel 1929 dal matematico belga Paul Poulet nel suo libro "La caccia ai numeri" con 62 nuove coppie di numeri amicabili, in totale Poulet ne scoprì 108. Un fatto curioso è che Fermat arrivò al suo teorema, il piccolo teorema di Fermat, proprio nel tentativo di trovare numeri amicabili. Infatti a questo scopo bisogna fattorizzare in prodotto di primi le somme dei divisori di numeri del tipo p^n. Essendo tale somma uguale a $\frac{p^n-1}{p-1}$, Fermat si domandò se $p^n - 1$ sia divisibile per $n + 1$, quando $n + 1$ è primo.

3.12 Distribuzione dei numeri primi

Concludiamo con qualche cenno sulla distribuzione dei numeri primi. La domanda "Quanti primi ci sono?" è del tutto naturale, ma posta così ha l'ovvia risposta, "infiniti", dovuta al teorema di Euclide. Cerchiamo allora di togliere la possibilità di "speculare" con l'infinito, chiedendo: quanti primi ci sono minori di n, dove n è un dato numero naturale $n > 1$. Denotiamo la quantità di questi primi con $\pi(n)$. Si ha

$$\pi(2) = 1, \qquad \pi(3) = \pi(4) = 2, \qquad \pi(5) = \pi(6) = 3,$$
$$\pi(7) = \pi(8) = \pi(9) = \pi(10) = 4, \qquad \pi(11) = \pi(12) = 5,$$
$$\pi(14) = \pi(15) = \pi(16) = \pi(17) = 6, \qquad \pi(18) = \pi(19) = 7,$$
$$\pi(20) = \pi(21) = \pi(22) = 8,$$

$$\pi(23) = \pi(24) = \pi(25) = \pi(26) = \pi(27) = \pi(28) = 9, \ldots.$$

Si vede che questa distribuzione è molto caotica, lunghi intervalli senza numeri primi si alternano a brevissimi intervalli tra due primi consecutivi a distanza 2, coppie di *primi gemelli* (non è noto se esistono infinite coppie di numeri primi gemelli). Tuttavia ci sono certe regole come mostra il seguente postulato.

Postulato di Bertrand. *Per ogni $n \in \mathbb{N}_+$ l'intervallo $[n, 2n]$ contiene almeno un numero primo.*

Più precisamente, si dimostra che per ogni $n \in \mathbb{N}$ maggiore di 1 l'intervallo $[n, 2n-2]$ contiene almeno un numero primo. Mentre da un teorema più preciso di Chebishev segue che esistono almeno due numeri primi p nell'intervallo $[n, 2n]$ per ogni $n \in \mathbb{N}$ maggiore di 1. Il postulato di Bertrand permette di dimostrare facilmente per induzione che se $p_1, p_2, \ldots, p_n, \ldots$ sono tutti i numeri primi in ordine crescente, allora $p_n < 2^n$. In altre parole, $\pi(2^n) \geq n$, che si potrebbe formulare anche come $\pi(m) \geq \log_2 m$.

Secondo un teorema profondo dimostrato da Pafnuti Lvovic Cebicev (1821-1894), il rapporto $\pi(n)/n$ che permette di parlare della densità dei numeri primi è circa $1/\log n$, qui il logaritmo è in base $e = \lim_n (1 + 1/n)^n$. In altre parole con la crescita di n i primi diventano più "rari". D'altra parte, è noto che per ogni n la somma di tutti i valori reciproci $1/p$, dove $p \leq n$ è primo, è maggiore di $\log \log n - 1$, che porge un'ulteriore dimostrazione del teorema di Euclide della non finitezza dei numeri primi.

Per il postulato di Bertrand ogni intervallo del tipo $[n, 2n-2]$ contiene almeno un numero primo. D'altra parte, ci sono intervalli arbitrariamente lunghi di numeri naturali consecutivi che non contengono numeri primi, si veda l'esercizio 3.30.

Si può osservare la distribuzione dei numeri primi limitandosi a specifiche progressioni aritmetiche. Si prova nell'esercizio 3.6 che ciascuna delle progressioni aritmetiche $3k + 2$, $4k + 3$ e $6k + 5$ contiene infiniti numeri primi. Per quanto riguarda le progressioni aritmetiche in generale, vale il seguente risultato.

Teorema 3.48. (Teorema di Dirichlet) *Siano a e b due numeri naturali coprimi. Allora esistono infiniti numeri primi della forma $ak + b$.*

Osserviamo che $ak + b$ non può essere primo se a e b non sono coprimi.

Leggermente di altra natura è la seguente congettura di Goldbach, che è rimasta aperta per oltre duecento anni.

Congettura di Goldbach. *Ogni numero pari maggiore di 3 è somma di due numeri primi.*

È stata dimostrata la forma più debole della congettura: *ogni numero dispari maggiore di 5 è somma di tre numeri primi.*

3.13 Somme di due quadrati

In questo paragrafo descriviamo i numeri che possono essere scritti come somma di due quadrati. Iniziamo con il teorema id Wilson.

Teorema 3.49. (Teorema di Wilson) *Sia p un numero primo. Allora vale*

$$(p-1)! \equiv_p -1 .$$

DIMOSTRAZIONE. Per ogni $1, 2, \ldots, p-1$ esiste un'unica soluzione della congruenza

$$ix \equiv_p 1, \tag{16}$$

compresa tra 1 e $p-1$ per il teorema 3.18. Denotiamo con i^* tale soluzione e osserviamo che vale $(i^*)^* = i$ per l'unicità. Verifichiamo quando si ha $i = i^*$ per $i = 1, \ldots, p-1$. Questo significa che $i^2 \equiv_p 1$, cioè p divide $(i^2-1) = (i-1)(i+1)$ quindi questo accade se e solo se $i = 1, p-1$. Pertanto se nel seguente prodotto per ogni $i = 2, \ldots, p-2$ "raggruppiamo" gli elementi in coppie del tipo $i \cdot i^* \equiv_p 1$, si ottiene

$$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv_p 1 \cdot (p-1) \equiv_p -1.$$

□

Lemma 3.50. *Sia p un numero primo del tipo $p = 4k+1$. Allora la congruenza*

$$x^2 \equiv_p -1$$

ha soluzione.

DIMOSTRAZIONE. Siano $A = \{1, 2, \ldots, \frac{p-1}{2}\}$ e $B = \{\frac{p+1}{2}, \frac{p+1}{2}+1, \ldots, p-1\}$. Allora l'applicazione $\varphi : A \to B$ definita da $\varphi(x) := p - x$ è una biezione. Pertanto avendo $\prod_{x \in A} x = (\frac{p-1}{2})!$, notiamo che

$$(p-1)! = \prod_{x \in A} x \cdot \prod_{y \in B} y = (\tfrac{p-1}{2})! \cdot \prod_{x=1}^{\frac{p-1}{2}} (p-x) \equiv_p$$

$$\equiv_p (-1)^{\frac{p-1}{2}} ((\tfrac{p-1}{2})!)^2 = ((\tfrac{p-1}{2})!)^2, \tag{17}$$

poiché $\frac{p-1}{2} = 2k$ è pari. Per il teorema di Wilson 3.49 abbiamo $(p-1)! \equiv_p -1$, quindi (17) porge una soluzione della congruenza $x^2 \equiv_p -1$ con $x = (\frac{p-1}{2})!$. □

Nel seguito descriveremo i numeri naturali che si possono presentare come somme di due quadrati di numeri naturali.

Lemma 3.51. *Se n ed m si possono scrivere come somma di due quadrati, allora anche mn si può scrivere come somma di due quadrati.*

DIMOSTRAZIONE. Se $n = a^2 + b^2$ ed $m = c^2 + d^2$, allora

$$nm = (ac + bd)^2 + (ac - bd)^2.$$

□

Proposizione 3.52. *Ogni numero del tipo* $n = 2^\delta p_1^{\sigma_1} p_2^{\sigma_2} \dots p_r^{\sigma_r}$, *dove* $p_1, p_2, \dots, p_r$ *sono primi del tipo* $p = 4k + 1$, *si può presentare come somma di due quadrati di numeri naturali.*

DIMOSTRAZIONE. Dimostriamo prima che se p è un primo del tipo $p = 4k + 1$ allora p si può presentare come somma di due quadrati. Per il lemma 3.50 esiste una soluzione s della congruenza $x^2 \equiv_p -1$. Scegliamo il numero naturale d con la proprietà $d < \sqrt{p} < d + 1$, questo è possibile poiché $\sqrt{p}$ non è intero. Allora

$$d^2 < p < (d+1)^2. \tag{18}$$

L'insieme delle coppie (a, b) con $a, b = 0, 1, 2 \dots, d$ ha $(d + 1)^2 > p$ elementi, quindi esistono due coppie diverse $(a, b) \neq (a_1, b_1)$ tali che $a - bs$ e $a_1 - b_1 s$ hanno lo stesso resto modulo p, cioè $a - bs \equiv_p a_1 - b_1 s$. Allora con $c = a - a_1$ e $e = b - b_1$ si ha

$$c - es \equiv_p 0. \tag{19}$$

Si noti che ora c ed e possono essere anche negativi, ma comunque $|c| \leq d$ e $|e| \leq d$, quindi (18) implica

$$c^2 < p \quad \text{e} \quad e^2 < p. \tag{20}$$

Moltiplicando entrambe le parti di (19) per $c + es$ si ha $c^2 - s^2e^2 \equiv_p 0$, ma per la scelta di s abbiamo anche $s^2 \equiv_p -1$. Quindi $c^2 + e^2 \equiv_p 0$. Ora (20) implica $c^2 + e^2 < 2p$, quindi $c^2 + e^2 = p$.

Si osservi che $2 = 1^2 + 1^2$ e pertanto ogni primo che compare nella fattorizzazione di n si può scrivere come somma di due quadrati. Si conclude applicando il lemma 3.51. □

Lemma 3.53. *Siano* a *e* b *numeri interi e sia* p *un numero primo del tipo* $p = 4k + 3$ *che divide* $a^2 + b^2$. *Allora* p *divide* a *e* p *divide* b. *In particolare:*

(a) p^2 *divide* $a^2 + b^2$;
(b) la congruenza $x^2 \equiv_p -1$ *non ha soluzione.*
(c) se p^{2s+1} *divide* $a^2 + b^2$ *per qualche* $s \in \mathbb{N}$, *allora anche* p^{2s+2} *divide* $a^2 + b^2$.

DIMOSTRAZIONE. Supponiamo che p non divida uno dei numeri a e b. Poiché p divide $a^2 + b^2$, risulta che p non divide né a né b. Allora, per il piccolo teorema di Fermat sia ha $a^{p-1} \equiv_p 1$ e $b^{p-1} \equiv_p 1$, quindi

$$a^{p-1} \equiv_p b^{p-1}. \tag{21}$$

La nostra ipotesi implica la congruenza $a^2 \equiv_p -b^2$. Elevando alla $2k + 1 = \frac{p-1}{2}$ si ha $a^{p-1} \equiv_p -b^{p-1}$. Sommando con (21) abbiamo $2a^{p-1} \equiv_p 0$, assurdo perché il numero primo p non divide né 2, né a^{p-1}.

Per concludere notiamo che (a) e (b) seguono immediatamente dal fatto che p divide a e p divide b. Per (c) si applichi (a) e si faccia induzione su s. □

Teorema 3.54. *Un numero del tipo*

$$n = 2^{\delta} p_1^{\sigma_1} p_2^{\sigma_2} \dots p_r^{\sigma_r} q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}, \tag{22}$$

dove $p_1, p_2, \dots, p_r$ *sono primi del tipo* $p = 4k + 1$ *e* $q_1, q_2, \dots, q_s$ *sono primi del tipo* $p = 4k + 3$ *si può presentare come somma di due quadrati di numeri naturali se e solo se* $\alpha_1, \alpha_2, \dots, \alpha_s$ *sono pari.*

DIMOSTRAZIONE. Se n è del tipo (22), allora $n = n_1 \cdot a^2$ dove n_1 ha la forma descritta nella proposizione 3.52, e quindi n_1 si può presentare come somma di due quadrati di numeri naturali. Di conseguenza anche n si può presentare come somma di due quadrati di numeri naturali. Se $n = x^2 + y^2$, allora n ha la forma (22) per il lemma 3.53. □

Si può provare che i numeri naturali n che non sono della forma $n = 4^a(8b + 7)$, con $a \geq 0, b \geq 0$ si possono scrivere come somma di tre quadrati e infine che ogni numero naturale si può scrivere come somma di quattro quadrati:

Teorema di Lagrange. *Ogni numero naturale si può scrivere come somma di quattro quadrati.*

3.14 Esercizi sull'aritmetica dei numeri interi

Esercizio 3.1 Dimostrare che l'insieme ordinato $(\mathbb{N}^*, |)$ è un reticolo. Si dica se è limitato.

Esercizio 3.2 Determinare i numeri primi minori di 250.

Esercizio 3.3 Se un numero intero $n > 0$ non è primo, dimostrare che n ha divisori primi p minori o uguali a $\sqrt{n}$ e che nel crivello di Eratostene, al passo corrispondente a p, si possono conoscere i numeri primi fino a $(p + 2)^2 - 1$, se p è un numero primo dispari.

Esercizio 3.4 Si verifichi che il polinomio $f(x) = x^2 - x + 17$ è un *generatore di primi*, cioè $f(x)$ è un primo per $x \in \mathbb{N}, x \leq 15$.

Esercizio 3.5 Trovare il massimo comun divisore d di 142 e 96 ed esprimerlo nella forma $d = 142u + 96v$. Lo stesso per 212 e 176.

Esercizio 3.6 * Si dimostri che esistono infiniti numeri primi della forma:

(a) $3k + 2$;
(b) $6k + 5$;
(c) $4k + 3$.

Esercizio 3.7 Scrivere in base 9 il numero 1153.

Esercizio 3.8 Per ogni intero $n \geq 0$, sia u_n la parte immaginaria della potenza n-esima del numero complesso $2+i$:

$$u_n = Im((2+i)^n).$$

Dimostrare che la successione $n \mapsto u_n$ verifica la relazione di ricorrenza

$$u_{n+2} = 4u_{n+1} - 5u_n.$$

Si determini la successione delle classi resto modulo 5 degli interi u_n, per $n = 0, 1, \ldots$. Si dimostri che nessuna potenza $(2+i)^n$, con esponente $n > 0$, è reale.

Esercizio 3.9 Trovare tutte le soluzioni in $\mathbb{Z}_{126}$ dell'equazione congruenziale

$$30x \equiv_{126} 42.$$

Esercizio 3.10 Trovare tutti gli interi positivi minori di 100 che soddisfano l'equazione congruenziale $17x \equiv_{29} 3$.

Esercizio 3.11 Risolvere le seguenti equazioni congruenziali:

(a) $4x \equiv_{17} -3$;
(b) $29x + 3 \equiv_{12} 0$;
(c) $3x - 8 \equiv_{13} 0$;
(d) $7x \equiv_{19} 4$;
(e) $37x \equiv_{117} 25$;
(f) $13x \equiv_{153} 178$;
(g) $18x \equiv_{51} 5$.

Esercizio 3.12 Si risolva il sistema di congruenze

$$x \equiv_3 2, \quad x \equiv_4 1 \quad \text{e} \quad x \equiv_5 3.$$

Esercizio 3.13 Si risolva il sistema di congruenze

$$x \equiv_5 2, \qquad x \equiv_6 2 \qquad \text{e} \quad x \equiv_4 0.$$

Esercizio 3.14 Sia p un primo dispari.

(a) Dimostrare che l'equazione congruenziale $x^2 \equiv_p 1$ ha esattamente due soluzioni in $\mathbb{Z}/p\mathbb{Z}$.
(b) Siano p, q due primi dispari distinti. Dimostrare che l'equazione $x^2 \equiv_{pq} 1$ ha esattamente 4 soluzioni.
(c) Risolvere la congruenza $x^2 \equiv_{35} 1$.

Esercizio 3.15 Determinare le ultime due cifre di 7^{1996} e le ultime tre cifre di 7^{1983}.

Esercizio 3.16 Dimostrare che, per ogni $n \in \mathbb{N}$, si ha:

(a) l'ultima cifra di 7^{4n+1} è 7;
(b) le ultime due cifre di 5^{n+2} sono 25;

(c) l'ultima cifra di 2^{4n+3} è 8;
(d) l'ultima cifra di 3^{4n+1} è 3;
(e) l'ultima cifra di 4^{2n+3} è 4;
(f) l'ultima cifra di 3^{4n+3} è 7;
(g) l'ultima cifra di 7^{4n+2} è 9;
(h) l'ultima cifra di 9^{2n+1} è 9;
(i) l'ultima cifra di 6^{n+1} è 6.

Esercizio 3.17 Dimostrare che 67, 97, 193 e 257 sono numeri primi. Calcolare

$$o_{17}(10), \qquad o_{67}(2), \qquad o_{97}(2), \qquad o_{193}(2), \qquad o_{257}(2).$$

Esercizio 3.18 * Dimostrare la formula

$$n = \sum_{d|n} \varphi(d).$$

Esercizio 3.19 Definiamo il seguente polinomio: $f_b(x) = x^2 - x + b$, con $b \in \mathbb{N}$ e $b > 1$. Allora $f_b(x)$ si dice un *polinomio di Eulero* se per ogni $x \in \mathbb{N}$, $x < b$ si ha che $f_b(x)$ è un numero primo. Poiché $f_b(-x+1) = f_b(x)$, anche tutti i valori $f_b(x)$ con $-b+1 < x < 0$, x intero, saranno primi. Dimostrare che

(a) se $f_b(x) = x^2 - x + b$ è un polinomio di Eulero, allora b è primo;
(b) per $b = 2, 3, 5, 11, 17, 41$ $f_b(x)$ è un polinomio di Eulero;
(c) per $b \leq 1000$ questi sono gli unici polinomi di Eulero.

Esercizio 3.20 Dimostrare che se 2^m+1 è primo, allora $m = 2^n$ per qualche numero naturale n.

Esercizio 3.21 Dimostrare che $F_{n+1} = (F_n - 1)^2 + 1$. Di conseguenza F_{n+1} è primo se non ha divisori primi p con $p < F_n - 1$.

Esercizio 3.22 Siano x, n, m numeri naturali maggiori di 0. Dimostrare che:

(a) $(x^n - 1) = (x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$;
(b) se m divide n, allora $(x^m - 1)$ divide $(x^n - 1)$;
(c) se $x^m - 1$ è primo, con $m \geq 2$, allora $x = 2$ e m è primo.

Esercizio 3.23 Sia $n > 3$ un numero naturale. Dimostrare che ci sono almeno $\log_2 n$ numeri primi nell'intervallo $[2, n]$.

Esercizio 3.24 Siano p ed n numeri primi. Se p divide un numero di Mersenne M_n, allora $p \equiv_n 1$.

Esercizio 3.25 Dimostrare che $M_{13} = 2^{13} - 1$ è un numero primo.

Esercizio 3.26 Siano a e b due numeri naturali coprimi. Dimostrare che se il prodotto è un quadrato perfetto, cioè coincide con il quadrato di un altro numero naturale, lo sono anche entrambi i fattori a e b.

Esercizio 3.27 Fattorizzare in prodotto di numeri primi i numeri 5!, 6!, 7!, 8!.

Esercizio 3.28 Determinare con quanti zeri terminano i numeri 10! e 20!.

Esercizio 3.29 (a) Sia $a = \overline{a_3 a_2 a_1 a_0}$ un numero naturale con quattro cifre decimali. Allora a è divisibile per 1001 precisamente quando $a_2 = a_1 = 0$ e $a_3 = a_0$. In tal caso a è divisibile anche per 7, 11 e 13. In particolare 2002 è divisibile per 7, 11 e 13; e l'anno futuro più vicino con questa proprietà è 3003.

(b) Sia $a = \overline{a_4 a_3 a_2 a_1 a_0}$ un numero naturale con cinque cifre decimali. Allora a è divisibile per 1001 precisamente quando $a_2 = 0$, $a_4 = a_1$ e $a_3 = a_0$. In tal caso a è divisibile anche per 7, 11 e 13.

(c) Sia $a = \overline{a_5 a_4 a_3 a_2 a_1 a_0}$ un numero naturale con sei cifre decimali. Allora a è divisibile per 1001 precisamente quando $\overline{a_5 a_4 a_3} = \overline{a_2 a_1 a_0}$. In tal caso a è divisibile anche per 7, 11 e 13.

Esercizio 3.30 Sia $n > 1$ un intero. Provare che nessuno degli $n - 1$ numeri consecutivi $n! + 2, n! + 3, \dots, n! + n$ è primo.

Esercizio 3.31 Si dimostri che ci sono infiniti numeri primi del tipo $4k + 1$ e infiniti numeri primi del tipo $8k + 1$.

Esercizio 3.32 Sia $p > 2$ un numero primo. Dimostrare che:

(a) se p divide $a^2 + 1$ per qualche numero intero a, allora p è del tipo $4k + 1$.
(b) se p divide $a^4 + 1$ per qualche numero intero a, allora p è del tipo $8k + 1$.

Esercizio 3.33 Sia $s > 1$ un intero. Si dimostri che ci sono infiniti numeri primi del tipo $2^s k + 1$.

Esercizio 3.34 Dimostrare che 6, 28 e 496 sono perfetti.

Esercizio 3.35 Si dimostri che ogni numero naturale $n > 0$ si può scrivere in modo unico nella forma $\sum_{i=1}^{n} c_i \cdot i!$, con $0 \leq c_i \leq i$.

Esercizio 3.36 Sia $b_0 = 1, b_1, b_2, \dots b_n, \dots$ una successione di numeri naturali con $b_n > 1$ per $n > 0$ e sia $M_k = b_0 \dots b_k$ per ogni $k \in \mathbb{N}$. Dimostrare che ogni numero naturale $n > 0$ si può scrivere in modo unico nella forma $\sum_{i=0}^{\infty} c_i \cdot M_i$ con $0 \leq c_i < b_{i+1}$.

Esercizio 3.37 * Dimostrare che per ogni numero $n \in \mathbb{N}_+$ i seguenti numeri numeri sono composti.

(a) $2^{10n+1} + 19$;
(b) $2^{4n+1} + 7$;
(c) $2^{2^{10n+1}} + 19$;
(d) $2^{2^{4n+1}} + 7$.

Esercizio 3.38 Dimostrare che ci sono infiniti numeri composti del tipo:

(a) $10^n + 3$;

(b) $(2^{2^n} + 1)^2 + 2$.

Esercizio 3.39 Dimostrare che nessuna potenza 3^k finisce con $\ldots 11$.

Esercizio 3.40 Risolvere le equazioni congruenziali:

(a) $102x \equiv_{21} 14$;
(b) $15x \equiv_{87} 122$;
(c) $402x \equiv_{57} 45$;
(d) $37x \equiv_{16} 14$;
(e) $82x \equiv_{13} 174$.

Esercizio 3.41 Dimostrare che:

(a) per k dispari, 7 divide $13^{k+1} - 1$;
(b) per k pari, 5 non divide $3^{k+1} - 1$;
(c) per k pari, 5 non divide $3^{k+1} + 1$;
(d) per k pari, 5 non divide $13^{k+1} - 1$;
(e) per k pari, 5 non divide $13^{k+1} + 1$.

Esercizio 3.42 Trovare i seguenti massimi comuni divisori

$$(2^{44} - 1, 2^{26} - 1), \quad (2^{52} - 1, 2^{39} - 1) \text{ e } (2^{63} - 1, 2^{36} - 1).$$

Esercizio 3.43 * Siano x, n, m numeri naturali maggiori di 1. Dimostrare che

$$(x^m - 1, x^n - 1) = x^{(m,n)} - 1.$$

Esercizio 3.44 Dimostrare che 59 divide $2^{29} + 1$.

Esercizio 3.45 Dimostrare che:

(a) 13 divide $2^{70} + 3^{70}$;
(b) $11 \cdot 31 \cdot 61$ divide $20^{15} - 1$.

Esercizio 3.46 Sia $a > 1$ un numero naturale. Trovare il resto di a^{100} modulo 125.

Esercizio 3.47 Sia p un primo dispari. Dimostrare che esiste un intero a tale che la congruenza $x^2 \equiv_p a$ non è risolubile.

Esercizio 3.48 Usando argomentazioni sulle congruenze, dimostrare che le seguenti equazioni diofantee non hanno soluzioni intere:

(a) $x^2 - 7y^2 = 14$;
(b) $x^3 + 15y^3 = 24$;
(c) $x^2 - 33y^2 = 13$.

Esercizio 3.49 Dimostrare che se p è primo e $p \equiv_3 2$, per ogni intero a la congruenza

$$x^2 - y^3 \equiv_p a$$

ha p soluzioni distinte.

Esercizio 3.50 Dimostrare che l'equazione

$$x^2 - y^2 = 6$$

non ha soluzioni intere. Dimostrare che per ogni primo p, la congruenza associata modulo p ha soluzione. Dimostrare che la congruenza associata modulo 4 non ha soluzione.

Esercizio 3.51 * Dimostrare che il numero

$$\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

non è mai intero.

Esercizio 3.52 Sia n un numero naturale dispari. Dimostrare che n divide $2^{n!} - 1$.

Esercizio 3.53 Sia n un numero naturale. Dimostrare che n divide $a^{n!} - 1$ se a è coprimo con n.

Esercizio 3.54 Sia $n > 0$ un numero naturale. Dimostrare che il numero

$$\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$$

non è mai intero.

Esercizio 3.55 * Trovare le ultime due cifre di

(a) 2^{999};
(b) a^2, dove a è un numero pari;
(c) $(\ldots(((7^7)^7)^7)^7\ldots)^7$ (7 compare n volte);
(d) $7^{7^{\cdot^{\cdot^{7}}}}$ (7 compare n volte).

Esercizio 3.56 Sia p un numero primo. Dimostrare che:

(a) p divide il coefficiente binomiale $\binom{p}{k}$ per ogni $0 < k < p$.
(b) $(x+y)^{p^s} \equiv_p x^{p^s} + y^{p^s}$ per ogni $x, y \in \mathbb{Z}$ e $s \in \mathbb{N}$;
(c) la massima potenza p^m con la quale p divide $n!$ è data da

$$m = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^k} \right\rfloor + \ldots.$$

Esercizio 3.57 Trovare con quanti zeri termina 2000!.

Esercizio 3.58 Dimostrare che il numero $((3!)!)!$ ha più di mille cifre decimali e trovare con quanti zeri termina questo numero.

Esercizio 3.59 * Se $n \in \mathbb{N}_+$, si provi che $(n!)^{(n-1)!}$ divide $(n!)!$.

Esercizio 3.60 Se $n \in \mathbb{N}$ è maggiore di 2, dimostrare che 2^n non divide $n!$.

Esercizio 3.61 Determinare i numeri $n \in \mathbb{N}_+$ tali che n non divide $(n-1)!$.

Esercizio 3.62 Sia $p > 2$ un numero primo. Dimostrare che:

(a) se $x \equiv_p y$ per $x, y \in \mathbb{Z}$, allora $x^p \equiv_{p^2} y^p$;
(b) se $x^p + y^p \equiv_p 0$ per $x, y \in \mathbb{Z}$, allora $x^p + y^p \equiv_{p^2} 0$.

Esercizio 3.63 Siano $m, p, a \in \mathbb{N}$, con $m \geq 1$ e p primo. Provare che

$$\binom{p^a m}{p^a} \equiv_p m.$$

Esercizio 3.64 Siano p un primo e $a \in \mathbb{Z}$. Se $a^p \equiv_p 1$, si provi che $a^p \equiv_{p^2} 1$.

Esercizio 3.65 Sia p un numero primo. Dimostrare che $\binom{p-1}{k} \equiv_p (-1)^k$ per ogni $0 < k < p$.

Esercizio 3.66 Sia p un primo. Dimostrare che ogni fattore primo q di $2^p - 1$ verifica $q > p$. Dedurre che esistono infiniti numeri primi.

Esercizio 3.67 Sia φ la funzione di Eulero. Si determinino tutti gli interi positivi n per i quali $\varphi(n) \leq 4$.

Esercizio 3.68 Sia φ la funzione di Eulero. Si dimostri che per ogni intero $n > 2$, $\varphi(n)$ è un numero pari.

Esercizio 3.69 Siano h, k interi positivi distinti. Dimostrare che i numeri

$$2^{2^h} + 1 \quad \text{e} \quad 2^{2^k} + 1$$

sono coprimi. Dedurre l'esistenza di infiniti numeri primi.

Esercizio 3.70 Si considerino le successioni a_n, b_n di numeri naturali

$$a_n = 2^n - 2, \qquad b_n = 2^n(2^n - 2).$$

Dimostrare che per ogni $n \geq 1$, i numeri a_n e b_n hanno gli stessi fattori primi. Dimostrare che anche i numeri $a_n + 1, b_n + 1$ hanno gli stessi fattori primi.

Strutture algebriche

Il primo paragrafo introduce i semigruppi, strutture algebriche con un'operazione binaria con la sola richiesta che sia associativa. Il secondo paragrafo è dedicato ai semigruppi con un elemento neutro, detti monoidi. Nel caso dei gruppi l'operazione è più ricca di proprietà: oltre all'elemento neutro si richiede anche l'esistenza di un inverso per ogni elemento. Il terzo e quarto paragrafo trattano di gruppi, anelli e campi. Nel quinto paragrafo si ricordano le principali definizioni e teoremi (senza dimostrazioni) riguardanti gli spazi vettoriali definiti sui campi, che si suppongono già noti dai corsi di geometria.

4.1 Semigruppi

Sia G un insieme. Un'*operazione binaria* su G è un'applicazione $\circ : G \times G \to G$. Se a e b sono elementi di G, l'immagine tramite $\circ$ della coppia (a, b) si dice *prodotto* di a e b e si indica con $a \circ b$. Per indicare le operazioni useremo di solito i simboli $\cdot$ e $+$. L'operazione $\cdot$ è *associativa* se vale $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per ogni a, b e c in G.

Definizione 4.1. Un *semigruppo* è una coppia $(S, \cdot)$ dove S è un insieme, detto *supporto* del semigruppo, $\cdot$ è un'operazione binaria associativa su S.

D'ora in poi, quando non sarà necessario specificare l'operazione, scriveremo S al posto di $(S, \cdot)$ e scriveremo semplicemente ab al posto di $a \cdot b$. Grazie alla proprietà associativa dell'operazione $\cdot$, possiamo pertanto denotare $a(bc)$ con abc. Per $n \in \mathbb{N}$, $n \geq 2$, possiamo definire per induzione il prodotto di n elementi $x_1, \ldots, x_n$ con $x_1 \ldots x_n = (x_1 \ldots x_{n-1})x_n$.

Definizione 4.2. La cardinalità dell'insieme S si indica con $|S|$ e si dice *ordine* di S. Un semigruppo si dice *finito* se il suo ordine è un numero naturale.

Per due elementi $a, b \in G$ si dice che a e b *commutano* (o sono *permutabili*) se $ab = ba$. Un semigruppo A si dice *abeliano* o *commutativo* se per ogni a, b in A risulta $ab = ba$.

Esempio 4.3. Esempi di semigruppi sono

$$(\mathbb{N},+),\quad (\mathbb{N},\cdot),\quad (\mathbb{Z},+),\quad (\mathbb{Z},\cdot),\quad (\mathbb{Q},+),\quad (\mathbb{Q},\cdot),$$

$$(\mathbb{R},+),\quad (\mathbb{R},\cdot),\quad (\mathbb{C},+),\quad (\mathbb{C},\cdot),\quad (\mathbb{Z}_m,+),\quad (\mathbb{Z}_m,\cdot)\ \text{per}\ m\in\mathbb{Z}.$$

Sia $\mathbb{Q}_+ = \{q \in \mathbb{Q} : q > 0\}$ l'insieme dei numeri razionali strettamente positivi; allora le coppie $(\mathbb{Q}_+,+)$ e $(\mathbb{Q}_+,\cdot)$ risultano semigruppi.

Sia $P = \{z \in \mathbb{Z} : z \text{ è pari}\}$. Allora $(P,+)$ e $(P,\cdot)$ sono semigruppi.

Tutti i semigruppi nell'esempio 4.3 sono commutativi. Vediamo alcuni esempi di semigruppi non commutativi.

Esempio 4.4. (a) Sia $X = \{x, y\}$; definiamo un prodotto $\cdot$ in X ponendo

$$x\cdot x = x\cdot y = x \quad \text{e} \quad y\cdot y = y\cdot x = y.$$

Allora $(X,\cdot)$ è un semigruppo non commutativo, in quanto $x\cdot y \neq y\cdot x$.

(b) Sia X un insieme non vuoto con $|X| \geq 2$ e sia X^X l'insieme di tutte le funzioni da X in X. Allora $(X^X,\circ)$ è un semigruppo, dove $\circ$ è la composizione di funzioni. Infatti la composizione di applicazioni è associativa per il lemma 1.20. Siano

$$a, b \in X, \quad a \neq b,$$

definiamo due funzioni $f, g \in X^X$ con $f(x) = a$ e $g(x) = b$ per ogni $x \in X$. Allora $f\circ g \neq g\circ f$ e $(X^X,\circ)$ è un semigruppo non commutativo.

(c) Sia $C = \{f : \mathbb{R} \to \mathbb{R} \text{ tale che } f \text{ è continua}\}$ e sia $\circ$ la composizione di funzioni. Allora $(C,\circ)$ è un semigruppo non commutativo. Le due funzioni costanti f_0 e f_1 che mandano ogni elemento in 0 e 1 rispettivamente non commutano.

La legge di cancellazione in un semigruppo. In un semigruppo $(S,\cdot)$ si dice che si può *cancellare l'elemento x di S a sinistra* in S se da $xb = xc$ segue sempre $b = c$ per ogni coppia di elementi $b, c \in S$. Analogamente, se da $bx = cx$ si conclude $b = c$ per ogni coppia di elementi $b, c \in S$, si dice che si può *cancellare x a destra*. Si dice che il semigruppo $(S,\cdot)$ soddisfa *la legge di cancellazione* se ogni elemento di S si può cancellare a destra e a sinistra.

Esempio 4.5. I semigruppi $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Z}_m,+)$, $(\mathbb{N}_+,\cdot)$ e $(\mathbb{Q}_+,\cdot)$ soddisfano la legge di cancellazione, ma i semigruppi $(\mathbb{N},\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},\cdot)$, $(\mathbb{Z}_m,\cdot)$ no.

Per un semigruppo $(S,\cdot)$ e un elemento $x \in S$ definiamo le potenze di x nel modo seguente. Poniamo $x^1 = x$ e per $n \in \mathbb{N}$ con $n > 1$ poniamo $x^n = x^{n-1}x$.

Un elemento b di un semigruppo si dice *idempotente* se $b = b^2$. In generale un semigruppo potrebbe non avere degli idempotenti, per esempio $(\mathbb{N}_+,+)$, ma ogni semigruppo finito ha almeno un idempotente, si veda l'esercizio 4.7.

4.2 Monoidi

Un semigruppo $(M, \cdot)$ si dice *monoide* se esiste un *elemento neutro* 1 di M, tale che

$$1 \cdot a = a \cdot 1 = a \text{ per ogni } a \in M. \tag{1}$$

L'elemento neutro 1 di un monoide M è unico. Infatti, se per qualche elemento e di M risulta $e \cdot a = a \cdot e = a$ per ogni a in M, allora $e = e \cdot 1 = 1$.

Questo suggerisce di considerare il monoide anche come una terna $(M, \cdot, 1)$ dove M è un insieme, $\cdot$ è un'operazione binaria su M e 1 è un elemento di M che verifica la proprietà (1).

Per comodità, d'ora in poi, quando non sarà necessario specificare l'operazione e l'elemento neutro, scriveremo M al posto di $(M, \cdot)$ o $(M, \cdot, 1)$.

Se $(S, \cdot, 1)$ è un monoide e $x \in S$ poniamo anche $x^0 = 1$.

In un monoide l'elemento neutro è ovviamente un idempotente. Il seguente lemma dimostra che per i semigruppi con la legge di cancellazione queste due proprietà coincidono.

Lemma 4.6. *Un elemento e di un semigruppo con la legge di cancellazione è idempotente se e solo se e è l'elemento neutro.*

DIMOSTRAZIONE. Sia $(S, \cdot)$ un semigruppo con la legge di cancellazione e sia e un idempotente di S. Allora per ogni $a \in S$ si ha $ae = ae^2$ in quanto $e = e^2$. Cancellando e a destra ricaviamo $a = ae$. Analogamente si prova che $ea = a$. Quindi e è l'elemento neutro. □

Esempio 4.7. Tra i semigruppi considerati negli esempi 4.3, risultano essere dei monoidi:

$$(\mathbb{N}, +, 0),\ (\mathbb{N}, \cdot, 1)\ (\mathbb{Z}, +, 0),\ (\mathbb{Z}, \cdot, 1),\ (\mathbb{Q}, +, 0),\ (\mathbb{Q}, \cdot, 1),\ (\mathbb{R}, +, 0),\ (\mathbb{R}, \cdot, 1),$$
$$(\mathbb{C}, +, 0),\ (\mathbb{C}, \cdot, 1),\ (\mathbb{N}_+, \cdot, 1),\ (\mathbb{Q}_+, \cdot, 1),\ (\mathbb{Z}_m, +, 0),\ (\mathbb{Z}_m, \cdot, 1).$$

Tra quelli dell'esempio 4.4, risultano essere dei monoidi $(X^X, \circ, id)$ e $(\mathcal{C}, \circ, id)$, dove id è la funzione identità cioè quella che manda ogni elemento di un insieme in se stesso.

Infine se definiamo

$$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}, \quad \mathbb{Q}^* = \mathbb{Q} \setminus \{0\},, \quad \mathbb{R}^* = \mathbb{R} \setminus \{0\},, \quad \mathbb{C}^* = \mathbb{C} \setminus \{0\},$$

allora le terne

$$(\mathbb{Z}^*, \cdot, 1), \quad (\mathbb{Q}^*, \cdot, 1), \quad (\mathbb{R}^*, \cdot, 1), \quad (\mathbb{C}^*, \cdot, 1)$$

sono dei monoidi.

Un altro esempio è dato dall'insieme dei numeri complessi di modulo 1: sia

$$\mathbb{S} = \{z \in \mathbb{C} : |z| = 1\},$$

allora la terna $(\mathbb{S}, \cdot, 1)$ è un monoide.

Esempio 4.8. Sia $(X, \leq)$ un reticolo. Possiamo considerare $\vee$ e $\wedge$ come operazioni binarie su X. Entrambe le operazioni sono associative. Quindi $(X, \vee)$ e $(X, \wedge)$ risultano semigruppi. Inoltre se il reticolo $(X, \leq)$ è limitato, allora $(X, \vee, 0)$ e $(X, \wedge, 1)$ risultano monoidi.

I semigruppi ottenuti in questo modo nell'esempio 4.8 sono commutativi e hanno tutti gli elementi idempotenti. Questo esempio assai generico permette di ottenere anche degli esempi più concreti come segue.

Esempio 4.9. Sia X un insieme, allora l'insieme $\mathcal{P}(X)$ delle parti di X risulta un monoide rispetto all'unione, con elemento neutro $\emptyset$ e risulta un monoide anche rispetto all'intersezione, con elemento neutro X. Infatti $\mathcal{P}(X)$ ordinato con l'inclusione è un reticolo limitato e quindi si applica l'esempio 4.8.

4.3 Gruppi

Definizione 4.10. Sia M un monoide. Un elemento $a \in M$ si dice *invertibile* se esiste un elemento $x \in M$ tale che $ax = xa = 1$.

L'inverso x dell'elemento a è univocamente determinato da a. Infatti, se vale

$$ax' = x'a = 1$$

per qualche elemento $x' \in G$, si ha, usando la proprietà associativa,

$$x = 1x = (x'a)x = x'(ax) = x'1 = x'.$$

L'unicità dell'elemento inverso x di a, determinato dalla proprietà $ax = xa = 1$, ci consente di indicarlo con a^{-1}.

Possiamo finalmente dare la definizione più importante di questo capitolo.

Definizione 4.11. Un monoide $(M, \cdot, 1)$ si dice un *gruppo* se ogni elemento di M è invertibile.

Denoteremo un gruppo con $(G, \cdot, 1)$ oppure con $(G, \cdot)$ o più semplicemente con G quando non sarà necessario evidenziare l'operazione del gruppo.

Un gruppo $(G, \cdot)$ si dice *abeliano*, se risulta abeliano come semigruppo, cioè se il prodotto $\cdot$ soddisfa la legge commutativa.

Teorema 4.12. *Ogni gruppo soddisfa la legge di cancellazione.*

DIMOSTRAZIONE. Se $ab = ac$ in un gruppo G, allora vale

$$b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = 1c = c.$$

Quindi si può cancellare a a sinistra. Analogamente si conclude che si può cancellare a a destra. □

Più in generale da $ab = cd$ si può dedurre, ragionando allo stesso modo, che $b = a^{-1}cd$ e $a = cdb^{-1}$.

Teorema 4.13. *Un monoide finito* $(M, \cdot, 1)$ *è un gruppo se e solo se soddisfa la legge di cancellazione.*

DIMOSTRAZIONE. Se $(M, \cdot, 1)$ è un gruppo, allora il teorema 4.12 garantisce che $(M, \cdot, 1)$ soddisfa la legge di cancellazione.

Supponiamo che $(M, \cdot, 1)$ soddisfi la legge di cancellazione. Per vedere che $(M, \cdot, 1)$ risulta un gruppo basta far vedere che ogni elemento $a \in M$ è invertibile. L'applicazione $f : M \to M$ definita da $f(x) = ax$ per ogni $x \in M$ risulta iniettiva. Infatti, se $f(x) = f(y)$, allora $ax = ay$ e per la legge di cancellazione possiamo concludere che $x = y$. Essendo M finito, l'applicazione f è anche suriettiva. Quindi esiste $x \in M$ tale che $ax = 1$. Allo stesso modo si vede che esiste $y \in M$ con $ay = 1$. Ora $x = x1 = x(ay) = (xa)y = 1y = y$, da cui $x = a^{-1}$ è l'inverso di a. □

Notazione additiva. In molti casi quando il gruppo G è abeliano, si usa anche la notazione additiva, come nell'esempio 4.3: l'operazione viene denotata con $+$. Ecco, per esempio, in notazione additiva:

(a) la legge associativa: $a + (b + c) = (a + b) + c$ per ogni a, b e c in G;
(b) la legge di cancellazione: $a + b = a + c$ implica $b = c$ e $b + a = c + a$ implica $b = c$ per ogni a, b e c in G;
(c) le potenze di $x \in G$ si chiamano *multipli* di x e si scrivono nx, ponendo

$$nx = (n - 1)x + x$$

e pertanto la formula dell'esercizio 4.1 diventa

$$(n + m)x = nx + mx;$$

(d) l'elemento neutro viene denotato con 0;
(e) l'elemento inverso di x viene denotato con $-x$ e chiamato *opposto di* x.

Quindi l'elemento neutro 0 di $(G, +)$ soddisfa $0 + a = a + 0 = a$ per ogni a in G. Allora l'opposto $-a$ di a è definito dalla proprietà $(-a) + a = a + (-a) = 0$. Per semplicità ometteremo le parentesi e scriveremo nel seguito $-a + b$ e $a - b$ al posto di $(-a) + b$ e $a + (-b)$.

Esempio 4.14. Tra i monoidi dell'esempio 4.7 sono gruppi $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$, $(\mathbb{Q}^*, \cdot, 1)$, $(\mathbb{Q}_+, \cdot, 1)$, $(\mathbb{R}^*, \cdot, 1)$, $(\mathbb{R}_+, \cdot, 1)$, $(\mathbb{C}^*, \cdot, 1)$, $(\mathbb{S}, \cdot, 1)$, $(\mathbb{Z}_m, +, [0]_m)$.

Inoltre, se p è un numero primo e $\mathbb{Z}_p^*$ è l'insieme delle classi $[k]_p \neq [0]_p$, allora il monoide $(\mathbb{Z}_p^*, \cdot, [1]_p)$ è un gruppo.

Tutti i gruppi dell'esempio 4.14 sono abeliani. È facile vedere che i monoidi $(\mathbb{N}, +, 0)$ e $(\mathbb{N}, \cdot, 1)$ non sono gruppi. Esempi di famiglie di gruppi non abeliani saranno forniti nell'esercizio 4.4, nel lemma 5.7 e nel paragrafo 5.6.

4.4 Anelli e campi

In questo paragrafo introduciamo il concetto di strutture algebriche con due operazioni che utilizzeremo nel paragrafo 5.6 dei gruppi lineari e nei successivi capitoli.

Definizione 4.15. Un *anello* è una terna $(A, +, \cdot)$ dove A è un insieme, $+$ e $\cdot$ sono operazioni binarie su A che verificano le seguenti proprietà:

1. la coppia $(A, +)$ è un gruppo abeliano con elemento neutro che denoteremo con 0;
2. l'operazione $\cdot$ è *associativa*, cioè $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per ogni a, b e c in A;
3. vale la legge *distributiva*, cioè $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$ per ogni a, b e c in A.

Definizione 4.16. Un anello $(A, +, \cdot)$ si dice

1. *unitario*, se il semigruppo $(A, \cdot)$ è un monoide;
2. *commutativo*, se il semigruppo $(A, \cdot)$ è commutativo;
3. un *dominio di integrità* o brevemente *dominio*, se è unitario e commutativo e nel semigruppo $(A \setminus \{0\}, \cdot)$ vale la legge di cancellazione;
4. un *corpo* o *anello con divisione* se $(A \setminus \{0\}, \cdot)$ è un gruppo;
5. un *campo* se è un corpo commutativo.

Denoteremo un anello $(A, +, \cdot)$ anche semplicemente con A.

Esempio 4.17. Esempi di anelli sono $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}_m, +, \cdot)$, mentre

$$(\mathbb{Q}, +, \cdot), \qquad (\mathbb{R}, +, \cdot), \qquad (\mathbb{C}, +, \cdot), \qquad (\mathbb{F}_p, +, \cdot)$$

sono esempi di campi.

Lo studio degli anelli e dei campi è oggetto dei capitoli 9, 10, 11 e 12.

Ricordiamo che una *matrice* è una tabella rettangolare costituita da elementi di uno stesso anello R, disposti secondo un certo numero di righe e un certo numero di colonne. In generale una matrice di m righe e n colonne si dice una matrice $m \times n$, viene indicata con $A = (a_{ij})$ e ha la seguente configurazione:

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

con $i = 1, 2..., m$ e $j = 1, 2, ..., n$ e $a_{ij} \in R$.

Denoteremo con $M_{m \times n}(R)$ l'insieme di tutte le matrici $m \times n$ ad elementi in R. Una matrice si dice *quadrata* se $m = n$, cioè se ha lo stesso numero di righe e di colonne. Denoteremo con $M_n(R)$ l'insieme delle matrici quadrate $n \times n$ ad elementi in R.

Esempio 4.18. Sia R un anello unitario e $M_n(R)$ l'insieme delle matrici quadrate $n \times n$ a elementi in R. Chiameremo *matrice nulla* la matrice 0_n avente tutti gli elementi uguali a 0, cioè $0_n = (a_{ij})$, in cui $a_{ij} = 0$ per ogni $i, j = 1, ..., n$. Chiameremo *matrice identica* la matrice $I_n = (a_{ij})$, in cui $a_{ij} = 0$ se $i \neq j$ e $a_{ii} = 1$, per ogni $i, j = 1, ..., n$.

Date due matrici $A = (a_{ij})$ e $B = (b_{ij})$ in $M_n(R)$, si definisce la somma $+$ ponendo $A + B = C = (c_{ij})$ dove $c_{ij} = a_{ij} + b_{ij}$. Si ha $A + 0_n = A$ per ogni $A \in M_n(R)$.

Date due matrici $A = (a_{ij})$ e $B = (b_{ij})$ in $M_n(R)$, si definisce un prodotto $\cdot$ "righe per colonne" nel modo seguente:

$$A \cdot B = C = (c_{ij}) \quad \text{dove} \quad c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj}.$$

A volte è comodo presentare l'operazione in una struttura algebrica tramite una tabella. Come esempio diamo la tabella delle due operazioni $+$ e $\cdot$ nel campo $(\mathbb{Z}_5, +, \cdot)$.

Tabella della $+$ in $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabella della $\cdot$ in $\mathbb{Z}_5$

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Supponiamo ora di avere due semigruppi G ed H. Come si possono costruire nuovi semigruppi a partire da G ed H? Si è visto che dati due insiemi possiamo costruire il prodotto cartesiano dei due insiemi. Quando questi due insiemi sono dotati anche di una operazione è possibile dotare l'insieme prodotto della stessa operazione, definendo l'operazione sul prodotto "componente per componente". Diamo la definizione precisa di quanto detto.

Teorema 4.19. *Siano $(G, \cdot)$ e $(H, \cdot)$ due semigruppi. Nel prodotto cartesiano $G \times H$ si introduce la seguente operazione:*

$$\textit{per } g, g_1 \in G,\ h, h_1 \in H, \textit{ poniamo } (g, h) \cdot (g_1, h_1) = (gg_1, hh_1).$$

Allora $(G \times H, \cdot)$ risulta un semigruppo, detto prodotto diretto di G e H.

(a) Se $(G, \cdot, 1_G)$ e $(H, \cdot, 1_H)$ sono monoidi, allora $(G \times H, \cdot, (1_G, 1_H))$ risulta un monoide.

(b) Se $(G, \cdot, 1_G)$ e $(H, \cdot, 1_H)$ sono gruppi, allora anche $(G \times H, \cdot)$ risulta un gruppo.

(c) Se $(G, +, \cdot)$ e $(H, +, \cdot)$ sono anelli, allora la terna $(G \times H, +, \cdot)$ risulta un anello, dove $(G \times H, +)$ e $(G \times H, \cdot)$ sono i prodotti diretti di $(G, +)$ e $(H, +)$, rispettivamente di $(G, \cdot)$ e $(H, \cdot)$.

DIMOSTRAZIONE. Verifichiamo che l'operazione $\cdot$ è associativa. Siano $g, g_1, g_2 \in G$ e $h, h_1, h_2 \in H$. Allora

$$((g,h)(g_1,h_1))(g_2,h_2) = (gg_1, hh_1)(g_2,h_2) = ((gg_1)g_2, (hh_1)h_2) =$$
$$= (g(g_1g_2), h(h_1h_2)) = (g,h)(g_1g_2, h_1h_2) = (g,h)((g_1,h_1)(g_2,h_2)).$$

(a) Verifichiamo che $(1_G, 1_H)$ è l'elemento neutro. Per ogni coppia (g,h) di $G \times H$ risulta

$$(1_G, 1_H)(g,h) = (1_G g, 1_H h) =$$
$$(g,h) = (g1_G, h1_H) = (g,h)(1_G, 1_H).$$

(b) Per ogni coppia $(g,h) \in G \times H$ la coppia (g^{-1}, h^{-1}) risulta l'inverso di (g,h):

$$(g^{-1},h^{-1})(g,h) = (g^{-1}g, h^{-1}h) = (1_G, 1_H) = (gg^{-1}, hh^{-1}) = (g,h)(g^{-1},h^{-1}).$$

(c) Infine, se $(G,+,\cdot)$ e $(H,+,\cdot)$ sono anelli, si verifica facilmente che vale la legge distributiva della somma rispetto al prodotto. Quindi $G \times H$ risulta un anello.
□

4.5 Spazi vettoriali

In questo paragrafo ricordiamo la definizione di spazio vettoriale e alcune sue importanti proprietà, senza alcuna dimostrazione, in quanto sono oggetto di studio di altri corsi. Diamo invece la definizione più generale di modulo su un anello commutativo con unità. Avremo prima bisogno di analizzare il concetto di operazione in una struttura algebrica.

Le strutture algebriche finora considerate avevano una o più operazioni binarie, definite come applicazioni $A \times A \to A$, dove A è l'insieme supporto della struttura algebrica. Tali operazioni si intendono come *operazioni interne*. Dato uno spazio vettoriale V sopra un campo K, il prodotto per uno scalare λ *fissato* è un esempio di operazione interna unaria, cioè ad un argomento, che ad ogni $v \in V$ mette in corrispondenza il vettore $\lambda v \in V$. Tuttavia avere tante operazioni interne, una per ogni scalare $\lambda \in K$, può creare confusione. Per questo si preferisce vedere la moltiplicazione per uno scalare λ come funzione di due argomenti, cioè come un'applicazione $* : K \times V \to V$. Questo suggerisce di definire il concetto di *operazione esterna* di un insieme V, solitamente dotato già di qualche struttura algebrica, come un'applicazione $* : A \times V \to V$, dove anche l'insieme A è solitamente dotato già di qualche struttura algebrica.

Definizione 4.20. Sia $(A,+,\cdot)$ un anello commutativo con unità e sia $(V,+)$ un gruppo abeliano. Sia $* : A \times V \to V$ un'operazione esterna di V che goda delle seguenti proprietà, per ogni $v_1, v_2, v \in V$ e $a, b \in A$:

1. $a * (v_1 + v_2) = a * v_1 + a * v_2$;
2. $(a + b) * v = a * v + b * v$;

3. $a * (b * v) = (a \cdot b) * v$;
4. $1 * v = v$.

Allora V si dice A-*modulo*.Nel caso in cui A sia un campo, V si dice *spazio vettoriale su A*.

Gli elementi di uno spazio vettoriale V su un campo K vengono anche chiamati *vettori*, gli elementi del campo K vengono chiamati *scalari* e la moltiplicazione $*$ si dice *moltiplicazione per scalare*. Ove non ci siano pericoli di confusione ometteremo i segni di moltiplicazione $\cdot$ e $*$. Ricordiamo le definizioni di combinazione lineare, vettori linearmente indipendenti e base di uno spazio vettoriale.

Definizione 4.21. - Si dice *combinazione lineare* dei vettori $v_1, \ldots, v_n$ ($n \in \mathbb{N}_+$) ogni vettore del tipo $a_1v_1 + a_2v_2 + \ldots + a_nv_n$, con $a_1, a_2, \ldots, a_n \in K$.

- Un insieme finito di vettori $v_1, \ldots, v_n$ si dice *linearmente indipendente* se per $a_1, \ldots, a_n \in K$

$$a_1v_1 + a_2v_2 + \ldots + a_nv_n = 0 \implies a_i = 0, \text{ per ogni } i = 1, \ldots, n.$$

  I vettori $v_1, \ldots, v_n$ si dicono *linearmente dipendenti* se l'insieme $v_1, \ldots, v_n$ non è linearmente indipendente.
- Un insieme finito di vettori $v_1, \ldots, v_n$ si dice *insieme di generatori* dello spazio vettoriale V se ogni vettore di V è combinazione lineare di $v_1, \ldots, v_n$.
- Un insieme di vettori $\mathcal{V} = \{v_i : i \in I\}$ si dice *linearmente indipendente* se ogni sottoinsieme finito di $\mathcal{V}$ è linearmente indipendente.
- Un insieme di vettori $\mathcal{V} = \{v_i : i \in I\}$ si dice *insieme di generatori* dello spazio vettoriale V se ogni vettore di V è combinazione lineare di un numero finito di vettori di $\mathcal{V}$.
- Uno spazio vettoriale si dice *finitamente generato* se ha un insieme di generatori finito.
- Una *base* è un insieme di vettori linearmente indipendente e generatori.
- In uno spazio vettoriale finitamente generato le basi hanno tutte lo stesso numero di vettori: questo numero si chiama *dimensione dello spazio* e si denota con $\dim(V)$.

Esempio 4.22. Sia $n \in \mathbb{N}$ e K un campo.

(a) Per ogni $n \in \mathbb{N}_+$ K^n risulta uno spazio vettoriale su K considerando su K^n la struttura di gruppo abeliano che risulta da $(K, +)^n$ e la moltiplicazione di un vettore $v = (x_1, x_2, \ldots, x_n) \in K^n$ per uno scalare $a \in K$ definita da

$$ax = (ax_1, ax_2, \ldots, ax_n).$$

Ora i vettori

$$e_1 = (1, 0, \ldots, 0, 0), \quad e_2 = (0, 1, 0, \ldots, 0, 0), \quad \ldots, \quad e_n = (0, 0, \ldots, 0, 1)$$

formano una base di K^n. Pertanto K^n ha dimensione n.

(b) Se lo spazio V non ha una base finita, V non è finitamente generato. Si può dimostrare anche in questo caso che esistono basi di V e hanno tutte la stessa cardinalità che sarà chiamata *dimensione di V*, si veda l'esercizio 4.19.

Esempio 4.23. Sia K un campo e $M_n(K)$ l'insieme delle matrici a coefficienti in K. Allora $M_n(K)$ è uno spazio vettoriale su K con la somma definita nell'esempio 4.18 e la moltiplicazione per uno scalare definita da

$$* : K \times M_n(K) \to M_n(K) \quad \text{con} \quad k * A = (ka_{ij})$$

per ogni $k \in K$ e $A = (a_{ij}) \in M_n(K)$. Per ogni coppia (i, j) con $i, j = 1, \dots, n$ definiamo la matrice $E_{ij} = (a_{lm})$ con $a_{lm} = 1$ se $(l, m) = (i, j)$ e $a_{lm} = 0$ se $(l, m) \neq (i, j)$, per ogni $l, m = 1, \dots, n$. Si verifica facilmente che una base di $M_n(K)$ su K è data dalle matrici E_{ij} con $i, j = 1, \dots n$; pertanto la dimensione dello spazio vettoriale $M_n(K)$ su K è n^2.

Come vedremo per le altre strutture algebriche possiamo definire anche in questo caso sottospazi, spazi quozienti e omomorfismi, con l'ovvio significato dei termini. Riportiamo per completezza tali definizioni.

Definizione 4.24. - Un sottoinsieme non vuoto W di uno spazio vettoriale V è un suo *sottospazio* se per ogni $v, w \in W$ e per ogni $a \in K$ si ha $v + w \in W$ e $av \in W$.
- Il più piccolo sottospazio che contiene un insieme X si dice *sottospazio generato da* X. Il *rango* di una famiglia di vettori di V è la dimensione del sottospazio vettoriale da essi generato.
- Se U e W sono sottospazi di V, si denota con $U + W$ il sottospazio generato da U e W.

L'intersezione di sottospazi vettoriali è ancora un sottospazio vettoriale, mentre l'unione non lo è. Vale il seguente teorema.

Teorema 4.25. (Teorema di Grassman) *Se U e W sono sottospazi di uno spazio vettoriale V di dimensione finita, allora*

$$\dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W).$$

Riportiamo anche le definizioni e i teoremi riguardanti gli omomorfismi di spazi vettoriali, cioè le applicazioni che rispettano la struttura, che, come è noto, si chiamano applicazioni lineari.

Definizione 4.26. Un'applicazione $f : V \to W$ tra due spazi vettoriali V e W sul campo K si dice *lineare* se $f(v + w) = f(v) + f(w)$ e $f(av) = af(v)$ per ogni $v, w \in V$ e $a \in K$.

Se $f : V \to W$ è un'applicazione lineare tra due spazi vettoriali V e W, l'antimmagine dell'elemento nullo 0_W tramite f si dice *nucleo di* f, si denota con $\ker f$ ed è un sottospazio vettoriale di V.

Teorema 4.27. *Se $f : V \to W$ è un'applicazione lineare di spazi vettoriali, allora* $\dim V = \dim(\ker f) + \dim(\mathrm{Im} f)$, *ove* $\mathrm{Im} f = f(V)$ *è l'immagine di V tramite f, ed è un sottospazio vettoriale di W.*

Lemma 4.28. *Sia A un anello unitario e sia K un sottocampo di A. Allora A è uno spazio vettoriale su K.*

DIMOSTRAZIONE. Ricordiamo che $(A, +)$ è un gruppo commutativo e definiamo l'operazione prodotto scalare $* : K \times A \to A$, $k * a = k \cdot a$. L'operazione è ben definita, in quanto K è un sottocampo di A e pertanto il prodotto $k \cdot a$ è un elemento di A e gode di tutte le proprietà necessarie per essere spazio vettoriale, che provengono dalle analoghe proprietà del prodotto in A. □

Infine un'ultima proprietà degli spazi vettoriali.

Teorema 4.29. *Se $v_1, ..., v_n$ è una base di uno spazio vettoriale V e $w_1, ..., w_n$ sono vettori di un altro spazio vettoriale W, allora esiste una ed una sola applicazione lineare $f : V \to W$ tale che $f(v_i) = w_i$ per ogni $i = 1, ..., n$.*

Questo teorema permette di verificare che la dimensione di uno spazio vettoriale di dimensione finita lo caratterizza a meno di applicazioni lineari biettive.

Sia K un campo. Ricordiamo che il determinante $\det(A)$ di una matrice $A = (a_{ij}) \in M_n(K)$, viene introdotto come un'applicazione $\det : M_n(K) \to K$. Per $n = 1$ si ha $\det(A) = a_{11}$, mentre nel caso $n = 2$ si pone

$$\det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

Per $n \geq 2$ si definisce la matrice $A_{ij} \in M_{n-1}(K)$ rimuovendo la i-esima riga e la j-esima colonna di A. L'elemento $C_{ij} = (-1)^{i+j} \det(A_{ij})$ di K è detto *(ij)-esimo co-fattore* di A. Si può ora definire $\det : M_n(K) \to K$ a partire da $\det : M_{n-1}(K) \to K$ usando la formula

$$\det(A) = a_{11}C_{11} + a_{21}C_{21} + \ldots + a_{n1}C_{n1},$$

dovuta a Laplace. Questa formula permette di sviluppare $\det(A)$ lungo la prima colonna. Vale una formula simile anche per la j-esima colonna

$$\det(A) = a_{1j}C_{1j} + a_{2j}C_{2j} + \ldots + a_{nj}C_{nj}.$$

Inoltre è possibile sviluppare $\det(A)$ anche lungo una riga, per esempio la i-esima:

$$\det(A) = a_{i1}C_{i1} + a_{i2}C_{i2} + \ldots + a_{in}C_{in}.$$

La funzione $\det : M_n(K) \to K$ ha le seguenti proprietà importanti che permettono di calcolarla con opportune *trasformazioni elementari* sulle righe (o le colonne) della matrice A dei seguenti tre tipi:

(a) se scambiamo due righe o due colonne di A, il determinante della matrice che risulta sarà $-\det(A)$;
(b) se moltiplichiamo tutti gli elementi di una riga (o colonna) di A per un elemento $c \in K$, allora il determinante della matrice che risulta sarà $c\det(A)$;

(c) se il multiplo di una riga (o colonna) di A mediante la moltiplicazione per un elemento $c \in K$ viene aggiunto ad un'altra riga (o colonna), il determinante della matrice che risulta resta $\det(A)$.

Da (a) segue che per una matrice A avente due righe (o colonne) uguali si ha $\det(A) = 0$. Da (b) si ricava facilmente che per una matrice A avente una riga (o colonna) che consiste solo di zeri si ha $\det(A) = 0$. Di conseguenza per calcolare il determinante di una matrice, si scelgono opportune trasformazioni elementari sulle righe o sulle colonne in modo da ottenere molti elementi uguali a zero.

Nell'esercizio 4.4, si dimostra che se K è un campo, allora $(M_n(K), \cdot)$ è un monoide. L'insieme degli elementi invertibili di $(M_n(K), \cdot)$ è un gruppo, come si dimostra in generale nell'esercizio 4.17.

Definizione 4.30. Il gruppo delle matrici quadrate $n \times n$ invertibili a coefficienti in un campo K si chiama *gruppo generale lineare su un campo di dimensione* n e si denota con $GL_n(K)$.

Dalla geometria è noto che $GL_n(K)$ è in corrispondenza biunivoca con il gruppo delle trasformazioni lineari biettive dello spazio vettoriale K^n. Inoltre è noto che una matrice A di $M_n(K)$ è invertibile se e solo se $\det(A)$ è invertibile o equivalentemente se $\det(A) \neq 0$. Un ultimo teorema di geometria che utilizzeremo è il seguente.

Teorema 4.31. (Teorema di Binet) *Siano* $A, B \in M_n(K)$. *Allora*

$$\det(AB) = \det(A)\det(B).$$

Un'immediata conseguenza del teorema di Binet è il seguente corollario:

Corollario 4.32. *Siano* $A, B \in GL_n(K)$. *Allora*

(a) $\det(A^{-1}) = \det(A)^{-1}$;
(b) $\det(A^{-1}BA) = \det(B)$.

DIMOSTRAZIONE. (a) Per il teorema di Binet, si ha

$$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}),$$

da cui l'asserto.

(b) Per il teorema di Binet, si ha

$$\det(A^{-1}BA) = \det(A^{-1})\det(B)\det(A) =$$

$$= \det(A)^{-1}\det(A)\det(B) = \det(B),$$

per il punto (a). □

4.6 Esercizi sulle strutture algebriche

Esercizio 4.1 Dimostrare che per un elemento x di un semigruppo S vale $x^{n+m} = x^n x^m$ per tutti i numeri naturali n, m.

Esercizio 4.2 Se e è un elemento idempotente in un semigruppo S, si dimostri che $e^n = e$ per ogni intero positivo n.

Esercizio 4.3 Si dimostri che:

(a) se S è l'insieme dei numeri complessi z con $|z| > 1$, allora $(S, \cdot)$ è un semigruppo ma non un monoide;
(b) se S è l'insieme dei numeri complessi z con $|z| \geq 1$, allora $(S, \cdot, 1)$ è un monoide con legge di cancellazione.

Esercizio 4.4 Sia K un campo e $n \in \mathbb{N}_+$. Si dimostri che:

(a) $(M_n(K), +, 0_n)$ è un monoide abeliano.
(b) $(M_n(K), \cdot)$ è un monoide con elemento identico la matrice I_n. Se $n > 1$, allora $M_n(K)$ non è abeliano.

Esercizio 4.5 Sia $(M, \cdot, 1)$ un monoide e sia S un sottoinsieme di M tale che $(S, \cdot)$ risulta un semigruppo e $1 \notin S$. Si può affermare che S non è un monoide?

Esercizio 4.6 Quali dei monoidi dell'esempio 4.9 soddisfano la legge di cancellazione?

Esercizio 4.7 * Dimostrare che ogni semigruppo finito contiene idempotenti.

Esercizio 4.8 * Dimostrare che ogni semigruppo finito S con la legge di cancellazione risulta un gruppo.

Esercizio 4.9 * Dimostrare che sull'insieme finito $S = \{a, b\}$ ci sono precisamente 8 strutture di semigruppo, di cui 6 abeliane e 2 non abeliane. Di queste solo 2 risultano gruppi.

Esercizio 4.10 Sia $(S, \cdot)$ un monoide. Per $a, b \in S$ poniamo $a|b$ se esiste $c \in S$ tale che $b = ac$. Dimostrare che:

(a) la relazione binaria $|$ è di preordine;
(b) se $(S, \cdot, 1)$ è un monoide con la legge di cancellazione e gli elementi diversi da 1 non sono invertibili, allora $|$ è un ordine e l'insieme ordinato $(S, |)$ ha un elemento minimo.

Esercizio 4.11 Sia G il prodotto cartesiano $\mathbb{Q} \times \mathbb{Z}^*$. Definiamo un'operazione su G nel modo seguente: $(q, m) \cdot (q', m') = (q + mq', mm')$. Si provi che $(G, \cdot)$ è un monoide e si calcolino gli elementi invertibili. Si dica se G è un gruppo e se G è abeliano.

Esercizio 4.12 Si dica quali dei seguenti monoidi sono dei gruppi:

$$(\{0\},+), \quad (\{0,1\},\cdot), \quad (\{1,-1\},\cdot), \quad (\mathbb{Q}_+,\cdot),$$

dove $\cdot$ è l'usuale moltiplicazione di $\mathbb{Q}$.

Esercizio 4.13 Si calcolino gli elementi invertibili dei seguenti monoidi e si dica se sono dei gruppi: $(\mathcal{P}(X), \cup)$, $(\mathcal{P}(X), \cap)$.

Esercizio 4.14 Sia G il prodotto cartesiano $\mathbb{Q}^* \times \mathbb{Q}$. Definiamo un'operazione su G nel modo seguente: $(a,b)\cdot(a',b') = (aa', ab' + b/a')$. Si provi che $(G,\cdot)$ è un gruppo e si dica se G è abeliano.

Esercizio 4.15 Sia $G = \{\text{funzioni } f : \mathbb{R} \to \mathbb{R}\}$. Si definisca la funzione somma $f+g$ ponendo $(f+g)(x) = f(x) + g(x)$. Si dimostri che $(G,+)$ è un gruppo abeliano.

Esercizio 4.16 Sia

$$G = \{f : \mathbb{R} \to \mathbb{R}, \text{ funzioni tali che } f(x) = ax + b;\ a, b \in \mathbb{R},\ a \neq 0\}.$$

Si dimostri che G è un sottoinsieme di $S_{\mathbb{R}}$, l'insieme di tutte le applicazioni biettive di $\mathbb{R}$ in sé. Si provi che G è un gruppo rispetto alla composizione di funzioni e si dica se G è abeliano.

Esercizio 4.17 Sia $(M,\cdot)$ un monoide. Sia $U(M) = \{u \in M : u \text{ è invertibile}\}$. Si dimostri che $(U(M),\cdot)$ è un gruppo.

Esercizio 4.18 Sia $(G,\cdot)$ un gruppo e sia $* : G \times G \to G$ l'operazione così definita: per ogni $a, b \in G$ sia $a * b := b \cdot a$. Si dimostri che $(G,*)$ è un gruppo in cui l'identità per $*$ coincide con l'identità per $\cdot$ e anche l'inverso di un elemento a rispetto all'operazione $*$ coincide con l'inverso di a rispetto all'operazione $\cdot$. Si osservi che $\cdot$ coincide con $*$ se il gruppo G è abeliano.

Esercizio 4.19 * Sia K un campo e sia V una spazio vettoriale su K. Dimostrare che esistono basi di V e tutte hanno la stessa cardinalità.

Esercizio 4.20 * Dare esempi di spazi vettoriali che non sono di dimensione finita.

5

Gruppi e sottogruppi

Questo capitolo pone la basi per lo studio dei gruppi. Il primo paragrafo contiene alcune proprietà immediate del calcolo con le potenze in un gruppo, mentre il secondo è dedicato all'esempio di gruppi *par excellence*, cioè i gruppi di permutazioni. Infatti ogni gruppo può essere visto come un gruppo di permutazioni.

Nel terzo paragrafo si espone il concetto fondamentale di sottogruppo: sottoinsieme del gruppo che risulta gruppo esso stesso se considerato con l'operazione ereditata dal gruppo. L'idea di introdurre i sottogruppi è di semplificare lo studio del gruppo perché i sottogruppi hanno spesso una struttura più semplice. Nel quarto paragrafo vengono introdotte due relazioni di equivalenza su G, le cui classi di equivalenza sono chiamate classi laterali. Il numero $[G : H]$ di queste classi laterali si calcola tramite la celebre formula $|G| = |H| \cdot [G : H]$, nota come teorema di Lagrange.

Il quinto paragrafo è dedicato ai sottogruppi normali N che hanno l'ulteriore proprietà che le due relazioni di equivalenza associate a N coincidono. Di conseguenza questa unica relazione è compatibile con l'operazione del gruppo. Questo permette l'introduzione, nel capitolo successivo, del gruppo quoziente avente come sostegno l'insieme quoziente G/N. I sottogruppi normali rappresentano l'analogo dei sottospazi degli spazi vettoriali. Inoltre, nel caso dei gruppi finiti, permettono di studiare la struttura di un gruppo tramite due gruppi di ordine più piccolo, N e G/N. Nel sesto paragrafo presentiamo i gruppi lineari, cioè i sottogruppi del gruppo delle trasformazioni lineari invertibili di uno spazio vettoriale. Introduciamo inoltre il gruppo dei quaternioni.

5.1 Proprietà elementari dei gruppi e primi esempi

Cominciamo con la regola di calcolo dell'inverso di un prodotto.

Lemma 5.1. *Sia G un gruppo e siano $a, b \in G$. Allora:*

(a) l'inverso del prodotto ab è l'elemento $b^{-1}a^{-1}$;
(b) a e b commutano se e solo se vale $a^{-1}b^{-1}ab = 1$;

(c) a e b commutano se e solo se $(ab)^{-1} = a^{-1}b^{-1}$.

DIMOSTRAZIONE. La dimostrazione è un facile esercizio. □

Per un gruppo $(G, \cdot)$ e un elemento $x \in G$ abbiamo già definito le potenze x^n per $n \in \mathbb{N}$. Ora per $n \in \mathbb{Z}$ con $n < 0$ poniamo $x^n = (x^{-1})^{-n}$. La formula $x^n = x^{n-1}x$ resta vera anche per gli interi $n < 0$:

$$x^n = (x^{-1})^{-n} = (x^{-1})^{-n}x^{-1}x = (x^{-1})^{-n+1}x = x^{n-1}x.$$

Osserviamo inoltre che $(x^{-1})^{-1} = x$ e che la formula $x^n = (x^{-1})^{-n}$ vale anche per $n \geq 0$. Possiamo ora provare le proprietà delle potenze.

Lemma 5.2. *Sia* $(G, \cdot)$ *un gruppo e* $x \in G$. *Allora per ogni coppia* $m, n \in \mathbb{Z}$ *vale:*

(a) $x^m x^n = x^{m+n}$;
(b) $(x^n)^{-1} = x^{-n}$ *e* $x^m x^n = x^n x^m$;
(c) $(x^m)^n = x^{mn}$.

DIMOSTRAZIONE. (a) Nel caso $n \geq 0$ proviamo per induzione su n che

$$x^m x^n = x^{m+n}$$

vale per ogni $m \in \mathbb{Z}$. Per $n = 0$ questo è ovvio. Supponiamo per ipotesi induttiva che $x^m x^{n-1} = x^{m+n-1}$ per ogni $m \in \mathbb{Z}$. Allora

$$x^m x^n = x^m x^{n-1}x = x^{m+n-1}x = x^{m+n}.$$

Nel caso $n < 0$, si ha

$$x^m x^n = (x^{-1})^{-m}(x^{-1})^{-n} = (x^{-1})^{(-m)+(-n)} = (x^{-1})^{(-(m+n))} = x^{m+n}.$$

(b) Segue immediatamente da (a).

(c) Nel caso $n \geq 0$ proviamo per induzione su n che $(x^m)^n = x^{mn}$ vale per ogni $m \in \mathbb{Z}$. Per $n = 0$ questo è ovvio. Per ipotesi induttiva si ha $(x^m)^{n-1} = x^{m(n-1)}$ per ogni $m \in \mathbb{Z}$. Allora

$$(x^m)^n = (x^m)^{n-1}(x^m) = (x^{m(n-1)})x^m = x^{m(n-1)+m} = x^{mn}.$$

Nel caso $n < 0$, si ha

$$(x^m)^n = ((x^m)^{-1})^{-n} = (x^{-m})^{-n} = x^{(-m)(-n)} = x^{mn}.$$ □

Osserviamo che se x ed y sono permutabili, allora anche x^{-1} ed y lo sono. Inoltre vale il seguente lemma.

Lemma 5.3. *Sia* $(G, \cdot)$ *un gruppo e* $x, y \in G$ *due elementi permutabili. Allora:*

(a) x^n *e* y *sono permutabili per ogni* $n \in \mathbb{Z}$;
(b) $(xy)^n = x^n y^n$ *per ogni* $n \in \mathbb{Z}$, *in particolare* $(xy)^{-1} = x^{-1}y^{-1}$;

(c) x^n e y^m sono permutabili per ogni $n, m \in \mathbb{Z}$.

DIMOSTRAZIONE. (a) Si dimostra prima per induzione che x^n e y sono permutabili per ogni $n \geq 0$ e con il lemma 5.2 (b) questo si estende per ogni $n \in \mathbb{Z}$.

(b) Per ogni $n \in \mathbb{N}$ si può dimostrare per induzione che vale $(xy)^n = x^n y^n$. Per $n < 0$ si applichi il lemma 5.2 (b).

(c) Per il punto (a), applicato ad x ed y, si ha che x^n e y sono permutabili. Applicando nuovamente il punto (a) ad y e $z = x^n$ si deduce che per ogni $m \in \mathbb{Z}$, x^n e y^m sono permutabili. □

Riformuliamo gli enunciati di questi due lemmi in notazione additiva. Innanzitutto per un gruppo abeliano $(G, +)$ e $x \in G$ introduciamo i *multipli* nx di x per ogni $n \in \mathbb{Z}$ come segue. Per $n \geq 0$ induttivamente, ponendo

$$0x = 0 \text{ e } nx = (n-1)x + x \text{ per } n > 0.$$

Per $n < 0$ si pone

$$nx = (-n)(-x).$$

Allora per ogni coppia $m, n \in \mathbb{Z}$ risulta

(a) $mx + nx = (m+n)x$;
(b) $-(nx) = (-n)x$;
(c) $n(mx) = nmx$;
(d) $n(x+y) = nx + ny$.

Definizione 5.4. Dato un gruppo G e un suo elemento x, consideriamo il seguente sottoinsieme dei numeri naturali $S(x) = \{n \in \mathbb{N}_+ : x^n = 1\}$. Se $S(x)$ non è vuoto, per il principio del buon ordinamento di $\mathbb{N}$, S ammette un minimo elemento non nullo, che denoteremo con $o(x)$ e chiameremo *ordine* (o *periodo*) di x. Se $S(x)$ è vuoto, definiamo $o(x) = \infty$. Se $o(x) = m$ allora si dice che x è *periodico* di periodo m, mentre se $o(x) = \infty$ si dice che x è *aperiodico*.

Osserviamo che l'unico elemento di periodo 1 è l'elemento neutro. Vogliamo ora provare alcune proprietà degli elementi periodici.

Lemma 5.5. *Sia G un gruppo e $x \in G$ tale che $o(x) = m$ è finito. Allora:*

(a) $x^k = 1$ per qualche $k \in \mathbb{Z}$ se e solo se m divide k;
(b) $x^n = x^k$ per $n, k \in \mathbb{Z}$ se e solo se $n \equiv_m k$;
(c) $o(x^k) = \frac{m}{(m,k)}$;
(d) $o(x^{-1}) = m$.

DIMOSTRAZIONE. (a) Se m divide k, allora $k = qm$, da cui $x^{qm} = (x^m)^q = 1$.

Viceversa sia $x^k = 1$ per qualche $k \in \mathbb{Z}$. Dividiamo k per m con resto e troviamo $q \in \mathbb{Z}$ e $0 \leq r < m$ tali che $k = qm + r$. Ora $1 = x^k = x^{qm+r} = x^{qm}x^r = x^r$. Se fosse $r > 0$, si avrebbe $r \in S(x)$ contraddicendo la minimalità di m. Pertanto $r = 0$ e m divide k.

(b) Da (a) segue

$$n \equiv_m k \iff n - k \equiv_m 0 \iff x^n = x^k.$$

(c) Se $d = (m, k)$, allora $m = dm_1$ e $k = dk_1$, con $(k_1, m_1) = 1$. Sia $s = o(x^k)$. Allora $(x^k)^s = x^{ks} = 1$ e da (a) si deduce che m divide ks. Di conseguenza dm_1 divide $dk_1 s$ e cancellando d concludiamo che m_1 divide $k_1 s$. Ora $(k_1, m_1) = 1$ implica che m_1 divide s. Poiché $(x^k)^{m_1} = x^{k_1 d m_1} = (x^m)^{k_1} = 1$, da (a) segue che s divide m_1 e quindi $s = m_1 = \frac{m}{(m,k)}$.

(d) Segue da (c). □

Per calcolare l'inverso di una potenza $b = a^k$ di un elemento a di ordine m basta risolvere la congruenza $kx \equiv_m 1$. Allora la potenza a^x coincide con b^{-1}.

In caso di notazione additiva avremo $kx = 0$ per un multiplo di x se e solo se $o(x)$ divide k.

5.2 Gruppi di permutazioni

In questo paragrafo vogliamo studiare i *gruppi di permutazioni*, detti anche *gruppi simmetrici*, cioè insiemi di applicazioni biettive su un insieme, che sono gruppi con l'operazione di composizione di applicazioni. Questi gruppi sono importanti perché sono esempi concreti di gruppi e ogni gruppo astratto si può immergere in un gruppo di permutazioni. Questo significa che, in modo opportuno, possiamo immaginare ogni gruppo astratto come un gruppo di permutazioni. Inoltre i gruppi simmetrici forniranno una famiglia di esempi di gruppi non abeliani.

Definizione 5.6. Sia X un insieme. Denotiamo con S_X l'insieme di tutte le *permutazioni* di X, cioè delle applicazioni biettive di X in sé.

Lemma 5.7. *Sia S_X l'insieme delle permutazioni su un insieme non vuoto X. Sia $\circ$ la composizione di applicazioni e id_X l'applicazione identica. Allora la terna $(S_X, \circ, id_X)$ è un gruppo; se $|X| > 2$, allora S_X non è abeliano.*

DIMOSTRAZIONE. Abbiamo già provato nell'esempio 4.4 che la composizione di applicazioni è associativa. Osserviamo che

$$(f \circ id_X)(x) = f(id_X(x)) = f(x) = id_X(f(x)) = (id_X \circ f)(x).$$

Poiché f è biettiva, esiste l'inversa f^{-1} tale che $f \circ f^{-1} = id_X = f \circ f^{-1}$ e f^{-1} è biettiva. Pertanto $(S_X, \circ, id_X)$ è un gruppo. Proviamo ora che, se $|X| \geq 3$, allora S_X non è abeliano.

Siano x, y, z tre elementi distinti di X. Definiamo l'applicazione $f : X \longrightarrow X$ tale che $f(x) = y$, $f(y) = x$ e $f(t) = t$ per ogni $t \in X \setminus \{x, y\}$. Sia g l'applicazione $g : X \to X$ tale che $g(x) = z$, $g(z) = x$ e $g(t) = t$ per ogni $t \in X \setminus \{x, z\}$.

Allora

$$(f \circ g)(x) = f(g(x)) = f(z) = z$$

mentre

$$(g \circ f)(x) = g(f(x)) = g(y) = y$$

con $y \neq z$. Pertanto $f \circ g \neq g \circ f$ e quindi S_X non è abeliano. □

Se X è finito e di cardinalità n, X si può identificare con l'insieme

$$I_n = \{1, 2, \dots, n\}.$$

Denotiamo pertanto $S_X = S_n$ e gli elementi di X con $1, 2, \dots, n$. Con queste notazioni, S_3 non è abeliano. Vedremo più avanti che S_3 è il più piccolo gruppo non abeliano e fornirà spesso un esempio (negativo) per mostrare che talune proprietà non valgono in generale. La cardinalità di S_n è $n!$, come provato nel corollario 1.44.

Possiamo rappresentare una permutazione di S_n nel modo seguente

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ f(1) & f(2) & \dots & f(i) & \dots & f(n) \end{pmatrix}.$$

Per una permutazione f di X con inversa f^{-1} definiamo anche le potenze negative ponendo

$$f^{-n} = (f^{-1})^n = (f^n)^{-1}$$

per $n \in \mathbb{N}$, cioè

$$x = f^n(y) \Longleftrightarrow y = f^{-n}(x).$$

Definizione 5.8. Data $f \in S_X$ definiamo il *supporto* di f come l'insieme degli elementi che non vengono fissati da f, cioè

$$\text{supp}(f) = \{x \in X : f(x) \neq x\}.$$

È chiaro che si ha $\text{supp}(f^{-1}) = \text{supp}(f)$.

Vediamo un esempio. Sia f la permutazione di S_{12} definita come segue:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 6 & 7 & 10 & 5 & 9 & 4 & 3 & 2 & 8 & 11 & 12 \end{pmatrix}.$$

Allora $\text{supp}(f) = \{2, 3, 4, 6, 7, 8, 9, 10\}$.

Definizione 5.9. Diremo che due permutazioni $f, g \in S_X$ sono *disgiunte* se

$$\text{supp}(f) \cap \text{supp}(g) = \emptyset.$$

Osserviamo che se $x \in \text{supp}(f)$, allora anche $f(x) \in \text{supp}(f)$. Infatti se $f(x)$ non appartenesse a $\text{supp}(f)$, allora $f(f(x)) = f(x)$, da cui dedurremmo, per l'iniettività di f, che $f(x) = x$, contro l'ipotesi.

Lemma 5.10. *Se f e g sono due permutazioni disgiunte, allora f e g commutano.*

DIMOSTRAZIONE. Se $x \in \operatorname{supp}(f)$, allora dall'ipotesi che f e g sono disgiunte deduciamo che $g(x) = x$. Quindi $(f \circ g)(x) = f(g(x)) = f(x)$ e anche $(g \circ f)(x) = g(f(x)) = f(x)$, in quanto dall'osservazione precedente il lemma sappiamo che anche $f(x) \in \operatorname{supp}(f)$. In modo del tutto analogo si prova che se $y \in \operatorname{supp}(g)$, allora

$$(f \circ g)(y) = f(g(y)) = g(y) = g(f(y)) = (g \circ f)(y).$$

Infine se

$$z \notin \operatorname{supp}(f) \cup \operatorname{supp}(g),$$

si ha

$$(f \circ g)(z) = f(g(z)) = f(z) = z = g(z) = g(f(z)) = (g \circ f)(z).$$

Concludiamo che f e g commutano. □

Data $f \in S_X$, definiamo una relazione in $\operatorname{supp}(f)$ nel modo seguente:

$$a \sim_f b \iff \text{esiste } i \in \mathbb{Z} \text{ tale che } b = f^i(a).$$

Allora $\sim_f$ è una relazione di equivalenza. Infatti è
riflessiva: $a = f^0(a) = id(a)$,
simmetrica: se $b = f^i(a)$ allora $a = f^{-i}(b)$,
transitiva: se $b = f^i(a)$ e $c = f^j(b)$ allora $c = f^j(b) = f^j(f^i(a)) = f^{i+j}(a)$.
Pertanto l'insieme $\operatorname{supp}(f)$ si ripartisce in classi di equivalenza rispetto a questa relazione.

Definizione 5.11. La classe di un elemento $a \in \operatorname{supp}(f)$ si dice l'*orbita* di a rispetto ad f e si denota

$$[a]_f = \{\ldots, f^{-i}(a), \ldots, f^{-1}(a), a, f(a), \ldots, f^i(a), \ldots\}.$$

Supponiamo ora che $\operatorname{supp}(f)$ sia finito e sia $a \in \operatorname{supp}(f)$; allora l'orbita di a rispetto ad f è finita e pertanto esistono due interi i, j con $i \neq j$ tali che

$$f^i(a) = f^j(a).$$

Possiamo supporre $i > j$ e applicando f^{-j} all'uguaglianza $f^i(a) = f^j(a)$, otteniamo $f^{i-j}(a) = a$. L'insieme $\mathcal{S} = \{n \in \mathbb{N}_+ : f^n(a) = a\}$ è non vuoto perché $i - j \in \mathcal{S}$, pertanto per il principio del minimo esiste un elemento minimo d. Allora gli elementi $a, f(a), \ldots, f^{d-1}(a)$ sono tutti distinti e sono contenuti in $[a]_f$. Sia ora $f^n(a) \in [a]_f$, $n \in \mathbb{Z}$. Per la divisione euclidea, esistono $q, r \in \mathbb{Z}$ tali che $n = qd + r$, con $0 \leq r < d$. È facile dimostrare per induzione che $f^{dq}(a) = a$ per ogni $q \in \mathbb{Z}$. Allora

$$f^n(a) = (f^r \circ f^{dq})(a) = f^r(f^{dq}(a)) = f^r(a) \in \{a, f(a), \ldots, f^{d-1}(a)\}.$$

Abbiamo così dimostrato che

$$[a]_f = \{a, f(a), \ldots, f^{d-1}(a)\}$$

per qualche $d \geq 2 \in \mathbb{N}$. Allora f ristretta a $[a]_f$ agisce *ciclicamente*, cioè manda $a_1 = a$ in $a_2 = f(a)$, a_2 in $a_3 = f(a_2)$, ... e infine manda $a_d = f^{d-1}(a)$ in $a_1 = a$. Motivati da questa osservazione definiamo un tipo relativamente semplice di permutazioni, ossia quelle che agiscono ciclicamente sul loro supporto.

Definizione 5.12. Sia $l > 1$, un *ciclo di lunghezza* l è una permutazione σ di X tale che se $\operatorname{supp}(\sigma) = \{a_1, \ldots, a_l\} \subseteq X$, allora $\sigma(a_i) = a_{i+1}$ per ogni $i = 1, \ldots, l-1$ e $\sigma(a_l) = a_1$. Un ciclo di lunghezza l si dice anche un l-ciclo. Un 2-ciclo si chiama anche *trasposizione*.

Denoteremo il ciclo σ con $(a_1 a_2 \ldots a_l)$ e notiamo subito che anche

$$(a_2 a_3 \ldots a_l a_1), \quad (a_3 a_4 \ldots a_l a_1 a_2), \text{ ecc.}$$

definiscono lo stesso ciclo σ.

Lemma 5.13. *Sia* $\sigma = (a_1 \ldots a_{l-1} a_l) \in S_n$, $n \in \mathbb{N}, n \geq 2$ *un ciclo di lunghezza* $l \geq 2$. *Allora:*

(a) $o(\sigma) = l$;
(b) $\operatorname{supp}(\sigma) = \operatorname{supp}(\sigma^j)$ *per ogni* $j \in \mathbb{Z}$ *e* $\sigma^j \neq id$;
(c) $\sigma^{-1} = (a_l a_{l-1} \ldots a_1)$.

DIMOSTRAZIONE. (a) Osserviamo che $\sigma^j(a_1) = a_{j+1}$, se $j = 1, \ldots, l-1$ con $a_{j+1} \neq a_1$, mentre $\sigma^l(a_1) = a_1$. Pertanto $o(\sigma) \geq l$. D'altro canto $\sigma^l(a_i) = a_i$ per ogni $i = 1, \ldots, l$, da cui $\sigma^l = id$ e $o(\sigma) = l$.

(b) Per il punto (a) non è restrittivo supporre $0 < j < l$. Se $x \notin \operatorname{supp}(\sigma)$, allora si ha banalmente $x \notin \operatorname{supp}(\sigma^j)$. Quindi $\operatorname{supp}(\sigma^j) \subseteq \operatorname{supp}(\sigma)$. Per dimostrare l'atra inclusione consideriamo $a_i \in \operatorname{supp}(\sigma^j)$. Allora $\sigma^j(a_i) = a_{i+j}$ se $i+j \leq l$, altrimenti $\sigma^j(a_i) = a_{i+j-l}$. In entrambi casi si ha $\sigma^j(a_i) \neq a_i$ per $0 < j < l$.

(c) Calcoliamo $\sigma \circ (a_l a_{l-1} \ldots a_1) = (a_l a_{l-1} \ldots a_1) \circ \sigma = id$. □

Dimostriamo ora come i cicli risultino essere gli "atomi" con cui costruire ogni permutazione.

Teorema 5.14. *Sia f una permutazione non identica di S_X con supporto finito. Allora f si scrive in modo essenzialmente unico come prodotto di cicli disgiunti.*

DIMOSTRAZIONE. Sia f una permutazione di S_X. Siano $[a_1]_f, \ldots, [a_t]_f$ le orbite di f su $\operatorname{supp}(f)$, di cardinalità rispettivamente $d_1, \ldots, d_t$, tutte maggiori di 1. Se denotiamo con $a_i^j = f^j(a_i)$, per $i = 1, \ldots, t$ e $j = 0, \ldots, d_i - 1$, abbiamo appena provato che $[a_i]_f = \{a_i^0, \ldots, a_i^{d_i-1}\}$ e che la restrizione di f al sottoinsieme $[a_i]_f$ di X coincide con il ciclo $(a_i^0 \ldots a_i^{d_i-1})$. Sia

$$g = (a_1^0 \ldots a_1^{d_1-1}) \circ \ldots \circ (a_t^0 \ldots a_t^{d_t-1});$$

allora, poiché le orbite costituiscono una partizione di $\mathrm{supp}(f) = \mathrm{supp}(g)$ e f coincide con g su ciascuna delle orbite, concludiamo che $f = g$. Osserviamo infine che i cicli $(a_i^0 \ldots a_i^{d_i-1})$, $i = 1, \ldots, t$ sono disgiunti, proprio perché le orbite costituiscono una partizione di $\mathrm{supp}(f)$. Pertanto questi cicli commutano. La costruzione dei cicli dimostra che sono univocamente determinati, a meno dell'ordine dei fattori. □

Quando una permutazione si scrive come prodotto di cicli disgiunti, spesso ometteremo di indicare il segno $\circ$ del prodotto tra l'uno e l'altro.

Osserviamo che se σ, τ sono due permutazioni di S_n, la scrittura $\sigma\tau$ sta ad indicare in questo libro $\sigma \circ \tau$. Tale scrittura non è però universalmente riconosciuta. Infatti in molti libri, soprattutto di teoria dei gruppi, $\sigma\tau$ sta ad indicare che si applica *prima* σ e *poi* τ.

È chiaro che nel caso in cui le due permutazioni σ e τ permutino, non è necessario fare questa distinzione, in quanto $\sigma \circ \tau = \tau \circ \sigma$.

Vediamo ora un paio di esempi.

Esempio 5.15. Scriviamo come prodotto di cicli disgiunti in S_7 le due seguenti permutazioni:

$$f = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 1\,6\,4\,5\,7\,2\,3 \end{pmatrix}, \quad g = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,3\,4\,1\,5\,6\,7 \end{pmatrix}.$$

Allora $f = (3457)(26)$ e $g = (1234)$.

Calcoliamo $f \circ g$. Osserviamo che 1 va in 2 tramite g e 2 va in 6 tramite f, da cui

$$f \circ g = (16\ldots)\ldots .$$

Ora 6 resta in 6 tramite g e va in 2 tramite f, da cui

$$f \circ g = (162\ldots).$$

Ora 2 va in 3 tramite g e 3 va in 4 tramite f,

$$f \circ g = (1624\ldots)\ldots .$$

Infine 4 va in 1 tramite g e 1 resta in 1 tramite f, cioè

$$f \circ g = (1624)\ldots .$$

Consideriamo ora l'immagine di 3: 3 va in 4 tramite g e 4 va in 5 tramite f, da cui

$$f \circ g = (1624)(35\ldots)\ldots .$$

Ora 5 resta in 5 tramite g e 5 va in 7 tramite f, da cui

$$f \circ g = (1624)(357\ldots)\ldots .$$

Infine 7 resta in 7 tramite g e va in 3 tramite f

$$f \circ g = (3457)(26) \circ (1234) = (1624)(357).$$

Esempio 5.16. Calcoliamo il prodotto di 3 permutazioni in S_7:

$$(1237) \circ (3245) \circ (53) = (537124).$$

Osservazione 5.17. Nell'esercizio 5.10 si dimostra che il periodo di una permutazione scritta come prodotto di cicli disgiunti è il minimo comune multiplo dei periodi dei cicli che la compongono. Da questo segue che una permutazione f ha ordine un primo p se e solo se si scrive come prodotto di cicli disgiunti tutti di lunghezza p.

Definizione 5.18. Siano $n \in \mathbb{N}$ con $n > 1$, $f \in S_n$ una permutazione non identica e $f = \sigma_1\sigma_2 \dots \sigma_t$ la sua fattorizzazione in cicli disgiunti, con σ_i ciclo di lunghezza l_i. Definiamo il numero intero

$$N(f) = (l_1 - 1) + (l_2 - 1) + \dots + (l_t - 1) = \sum_{i=1}^{t}(l_i - 1) = \sum_{i=1}^{t} l_i \; - \; t.$$

Se $f = id$, poniamo $N(id) = 0$.

Definiamo $\text{sgn}(f) = (-1)^{N(f)}$ il *segno* di una permutazione. Una permutazione f si dice di *classe pari* o *dispari* a seconda che $N(f)$ sia pari o dispari o, equivalentemente, $\text{sgn}(f) = 1$ o -1.

Sia ora $(a_1a_2 \dots a_l)$ un ciclo di lunghezza l. Allora

$$(a_1a_2 \dots a_l) = (a_1a_l) \circ (a_1a_{l-1}) \circ \dots \circ (a_1a_3) \circ (a_1a_2).$$

Poiché ogni permutazione è prodotto di cicli, proviamo:

Lemma 5.19. *Ogni permutazione f si può scrivere come prodotto di $N(f)$ trasposizioni.*

DIMOSTRAZIONE. Osserviamo che un ciclo di lunghezza l si scrive come il prodotto di $l-1$ trasposizioni. Quindi una permutazione $f = \sigma_1\sigma_2 \dots \sigma_t$ scritta come prodotto di cicli disgiunti, con σ_i ciclo di lunghezza l_i, si può scrivere come prodotto di $N(f)$ trasposizioni. □

Vediamo un esempio di come si possa scrivere una permutazione come prodotto di cicli disgiunti e di come calcolare $N(f)$.

Esempio 5.20. Consideriamo la seguente permutazione f di S_9:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 7 & 5 & 6 & 9 & 8 & 3 & 1 \end{pmatrix}$$

Allora $f = (124569)(378)$ è la fattorizzazione di f in cicli disgiunti e

$$N(f) = (6 - 1) + (3 - 1) = 7$$

e quindi f è dispari. Infine

$$f = (124569)(378) = (19)(16)(15)(14)(12)(38)(37)$$

è una fattorizzazione di f come prodotto di trasposizioni.

Osserviamo che se f, g sono due permutazioni disgiunte, allora

$$N(f \circ g) = N(f) + N(g)$$

perché la fattorizzazione in cicli disgiunti di $f \circ g$ è semplicemente il prodotto delle rispettive fattorizzazioni.

Diamo alcune regole per il calcolo di $N(\sigma \circ \rho)$ con σ, ρ cicli non disgiunti. Cominciamo con il caso in cui l'intersezione dei supporti sia la più piccola possibile. Sia $\sigma = (a_1 \dots a_m)$ e supponiamo $|\text{supp}(\sigma) \cap \text{supp}(\rho)| = 1$. Possiamo supporre $\rho = (a_m b_1 \dots b_l)$, $b_i \neq a_j$ per ogni $i = 1, \dots, l$ $j = 1, \dots, m$. Allora

$$\sigma \circ \rho = (a_1 \dots a_m b_1 \dots b_l). \tag{1}$$

Si deduce che

$$N(\sigma \circ \rho) = m + l - 1 = (m - 1) + (l + 1 - 1) = N(\sigma) + N(\rho).$$

Nel caso in cui ρ sia una trasposizione, possiamo supporre $\rho = (a_m a_{m+1})$, da cui $\sigma \circ \rho = (a_1 ... a_m a_{m+1})$.

Deduciamo da questa uguaglianza che se $\sigma = (a_1 a_2 \dots a_m)$, si ha

$$\sigma = (a_1 a_2 \dots a_m) = (a_1 a_2 \dots a_{m-1}) \circ (a_{m-1} a_m) =$$

$$(a_1 a_2 \dots a_{m-2}) \circ (a_{m-2} a_{m-1}) \circ (a_{m-1} a_m) =$$

$$= \dots = (a_1 a_2) \circ (a_2 a_3) \circ \dots \circ (a_{m-2} a_{m-1}) \circ (a_{m-1} a_m).$$

Consideriamo ora il caso in cui $|\text{supp}(\sigma) \cap \text{supp}(\tau)| = 2$. Se $\tau = (a_{m-1} a_m)$, allora $\sigma \circ \tau = (a_1 \dots a_m) \circ (a_{m-1} a_m) = (a_1 \dots a_{m-1})$.

Anche in questo caso

$$N(\sigma \circ \tau) = m - 1 - 1 = m - 2 = N(\sigma) - N(\tau).$$

Se $\tau = (a_i a_m)$, $i < m - 1$, allora

$$\sigma \circ \tau = (a_1 \dots a_i \dots a_m) \circ (a_i a_m) = (a_1 \dots a_i)(a_{i+1} \dots a_m).$$

In questo caso

$$N(\sigma \circ \tau) = (i - 1) + (m - i - 1) = m - 2 = N(\sigma) - N(\tau).$$

Abbiamo così provato il seguente lemma.

Lemma 5.21. *Se σ è un ciclo e τ è una trasposizione, si ha*

$$N(\sigma \circ \tau) = N(\sigma) \pm N(\tau) \equiv_2 N(\sigma) + N(\tau).$$

Ora possiamo provare che il segno è una funzione moltiplicativa da S_n a $\{1, -1\}$.

Lemma 5.22. *Siano $f, g \in S_n$. Allora* $\text{sgn}(f \circ g) = \text{sgn}(f)\,\text{sgn}(g)$.

DIMOSTRAZIONE. Dapprima proviamo il lemma nel caso in cui g sia una trasposizione. Sia dunque $g = (ab)$. Scriviamo

$$f = f_1 \dots f_t$$

come prodotto di cicli disgiunti, supponendo di mettere alla fine i cicli il cui supporto contiene a e b. Siano $l_1, \dots, l_t$ le lunghezze dei cicli f_i. Se $\{a, b\} \cap \operatorname{supp}(f) = \emptyset$, allora

$$N(f \circ g) = N(f) + 1.$$

Se $|\operatorname{supp}(f) \cap \operatorname{supp}(g)| = 1$, possiamo supporre $|\operatorname{supp}(f_t) \cap \operatorname{supp}(g)| = 1$, da cui per il lemma 5.21, si ha

$$N(f_t \circ g) = N(f_t) + N(g), \quad \text{da cui } N(f \circ g) = N(f) + N(g).$$

Se $a, b \in \operatorname{supp}(f)$, si possono avere due casi: a e b stanno nel supporto di un unico ciclo, oppure a e b stanno nel supporto di due cicli disgiunti. Nel primo caso possiamo supporre $|\operatorname{supp}(f_t) \cap \operatorname{supp}(g)| = 2$, da cui per il lemma 5.21

$$N(f_t \circ g) = N(f_t) - N(g) \implies N(f \circ g) = N(f) - N(g).$$

Nel secondo caso possiamo supporre

$$|\operatorname{supp}(f_t) \cap \operatorname{supp}(g)| = 1 \quad \text{e} \quad |\operatorname{supp}(f_{t-1}) \cap \operatorname{supp}(g)| = 1.$$

Allora, se $\sigma = f_t \circ g$, σ è un ciclo di lunghezza $l_t + 1$ e $N(\sigma) = N(f_t) + 1$ e inoltre $|\operatorname{supp}(f_{t-1}) \cap \operatorname{supp}(\sigma)| = 1$. Quindi per (1) si ha

$$N(f_{t-1} \circ \sigma) = N(f_{t-1}) + N(\sigma).$$

Essendo la permutazione $f_{t-1} \circ \sigma$ disgiunta dalle permutazioni $f_1, f_2, \dots, f_{t-2}$, si ricava

$$\begin{aligned} N(f \circ g) &= N(f_1 \circ \dots \circ f_{t-1} \circ \sigma) = \\ &= N(f_1) + \dots + N(f_{t-2}) + N(f_{t-1}) + N(\sigma) = \\ &= N(f_1) + \dots + N(f_{t-2}) + N(f_{t-1}) + N(f_t) + 1 = N(f) + N(g). \end{aligned}$$

Si conclude che

$$N(f \circ g) = N(f) \pm N(g)$$

e quindi

$$\operatorname{sgn}(f \circ g) = -\operatorname{sgn}(f) = \operatorname{sgn}(f) \operatorname{sgn}(g).$$

Sia ora g una qualsiasi permutazione: possiamo scrivere g come prodotto di $N(g)$ trasposizioni: $g = \tau_1 \circ \tau_2 \circ \dots \circ \tau_{N(g)}$ e facciamo induzione su $N(g)$. Allora

$$\operatorname{sgn}(f \circ g) = \operatorname{sgn}((f \circ \tau_1 \circ \tau_2 \circ \dots) \circ \tau_{N(g)})$$

che, per il caso appena dimostrato di una sola involuzione, permette di scrivere

$$\operatorname{sgn}(f \circ \tau_1 \circ \tau_2 \circ \dots) \operatorname{sgn}(\tau_{N(g)}),$$

da cui per ipotesi induttiva

$$\operatorname{sgn}(f \circ g) = \operatorname{sgn}(f) \operatorname{sgn}(\tau_1) \dots \operatorname{sgn}(\tau_{N(g)}) =$$

$$= \operatorname{sgn}(f)(-1)^{N(g)} = \operatorname{sgn}(f) \operatorname{sgn}(g).$$

□

Possiamo quindi affermare che una permutazione è di classe pari se e solo se si può scrivere come prodotto di un numero pari di trasposizioni.

5.3 Sottogruppi

Definizione 5.23. Un sottoinsieme non vuoto H di un gruppo G si dice *sottogruppo* se:

(S1) H è *stabile*, cioè $xy \in H$ per ogni coppia di elementi $x, y \in H$;
(S2) se $x \in H$, allora anche $x^{-1} \in H$.

Un sottogruppo H di G si dice *proprio* se $H \neq G$. Per indicare che H è un sottogruppo di G scriveremo $H \leq G$, nel caso in cui H è proprio scriveremo $H < G$.

Chiaramente $1 \in H$ per ogni sottogruppo H, poiché (S1) implica $1 = xx^{-1} \in H$ per ogni elemento $x \in H$ in quanto $x^{-1} \in H$ per (S2).

Esempio 5.24. Ci sono sempre i sottogruppi $G \leq G$ e $\{1\} \leq G$, che chiameremo ***banali***. In certi casi non ci sono sottogruppi non banali, come vedremo nel lemma 5.60 per il gruppo $(\mathbb{Z}_p, +)$, con p primo.

I sottogruppi di un gruppo G sono precisamente i sottoinsiemi H di G che risultano dei gruppi con la *stessa* operazione di G, cioè con la restrizione dell'operazione di G ad H. Di conseguenza l'operazione del sottogruppo H ha le stesse proprietà di quella di G: ad esempio se G è abeliano, anche il suo sottogruppo H lo è.

Vediamo ora qualche esempio di sottogruppo. Iniziamo con gli esempi numerici, la cui dimostrazione è un facile esercizio.

Esempio 5.25. Alcuni sottogruppi del gruppo additivo dei numeri complessi sono:

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +).$$

E alcuni sottogruppi del gruppo moltiplicativo dei numeri complessi non nulli sono:

$$(\mathbb{Q}^*, \cdot) \leq (\mathbb{R}^*, \cdot) \leq (\mathbb{C}^*, \cdot) \text{ e anche } (\mathbb{S}, \cdot) \leq (\mathbb{C}^*, \cdot).$$

Infine $(\mathbb{Z}^*, \cdot)$ eredita il prodotto per esempio da $(\mathbb{Q}^*, \cdot)$ ma, pur essendo stabile rispetto alla moltiplicazione, non è un sottogruppo di $(\mathbb{Q}^*, \cdot)$, in quanto gli unici elementi invertibili sono $1, -1$.

Vediamo ora alcuni esempi di sottogruppi di un gruppo non abeliano.

Esempio 5.26. Sia S_X il gruppo delle permutazioni su un insieme X. Sia $A \subseteq X$ e sia

$$H = \{f \in S_X : f(a) = a \text{ per ogni } a \in A\}.$$

Allora H è un sottogruppo. Infatti l'identità appartiene ad H, che pertanto non è vuoto. Inoltre se $f, g \in H$, si ha $(f \circ g)(a) = f(g(a)) = f(a) = a$ per ogni $a \in A$, da cui segue che $f \circ g \in H$. Infine se $f \in H$ e $a \in A$, si ha $a = f(a)$, da cui, applicando f^{-1}, $f^{-1}(a) = f^{-1}(f(a)) = (f^{-1} \circ f)(a) = id(a) = a$. Concludiamo che anche f^{-1} appartiene ad H.

Lemma 5.27. *Sia S_n il gruppo delle permutazioni su un insieme con n elementi. Allora l'insieme $A_n = \{f \in S_n : f \text{ è di classe pari}\}$ è un sottogruppo di S_n.*

DIMOSTRAZIONE. Innanzitutto A_n non è vuoto, perché l'identità ha classe pari. Se f e g sono due permutazioni di classe pari, allora anche $f \circ g$ è di classe pari, come dimostrato nel lemma 5.22. Se

$$f = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_t$$

è la fattorizzazione di f in cicli disgiunti,

$$f^{-1} = \sigma_1^{-1} \circ \sigma_2^{-1} \ldots \circ \sigma_t^{-1}$$

è la fattorizzazione di f^{-1} in cicli disgiunti perché i cicli σ_i permutano a due a due. Poiché la lunghezza di σ_i^{-1} coincide con la lunghezza di σ_i, si ha $N(f) = N(f^{-1})$.
□

Definizione 5.28. Il sottogruppo A_n si chiama *gruppo alterno* su n elementi.

Il lemma seguente fornisce un criterio per verificare se un sottoinsieme è un sottogruppo.

Lemma 5.29. *Un sottoinsieme non vuoto H di un gruppo G è un sottogruppo se e solo se*

$$x^{-1}y \in H \text{ per ogni coppia di elementi } x, y \in H. \quad (2)$$

DIMOSTRAZIONE. Sia $H \leq G$. Se $x, y \in H$, allora $x^{-1} \in H$ per (S2) della definizione 5.23 e quindi $x^{-1}y \in H$ per (S1).

Supponiamo che valga (2). Essendo H non vuoto esiste almeno un elemento $x_0 \in H$; applicando (2) a x_0 ed x_0, ricaviamo $1 = x_0^{-1}x_0 \in H$. Sia $x \in H$, applicando (2) ad x e 1 troviamo $x^{-1} = x^{-1}1 \in H$. Siano $x, y \in H$, per la proprietà (S2) della definizione 5.23 già verificata, vale $x^{-1} \in H$. Dalla (2) applicata a x^{-1} e y ricaviamo $xy = (x^{-1})^{-1}y \in H$. □

Utilizziamo il lemma 5.29 per provare che l'intersezione di sottogruppi è un sottogruppo.

Lemma 5.30. *L'intersezione di una famiglia qualsiasi di sottogruppi di un gruppo G è ancora un sottogruppo di G.*

DIMOSTRAZIONE. Sia $\{H_i\}_{i \in I}$ una famiglia di sottogruppi del gruppo G e sia

$$H = \bigcap_{i \in I} H_i.$$

Allora $1 \in H_i$ per ogni $i \in I$, quindi $1 \in H$. Per $x, y \in H$ si ha $x, y \in H_i$ per ogni $i \in I$. Quindi (2) implica $x^{-1}y \in H_i$ per ogni $i \in I$. Di conseguenza $x^{-1}y \in H$. Per il lemma 5.29 H è un sottogruppo. □

Se X è un sottoinsieme di G, l'intersezione di tutti i sottogruppi di G contenenti X è un sottogruppo di G che si chiama *sottogruppo generato da* X e si denota con $\langle X \rangle$. Chiaramente $\langle X \rangle$ è *il più piccolo sottogruppo di G contenente X.*

In particolare, se $G = \langle X \rangle$, diremo che X è un *sistema di generatori* di G oppure che G è *generato* da X. Inoltre, per alleggerire la notazione, se X è un insieme finito $X = \{x_1, x_2, \ldots, x_n\}$, si scrive $\langle X \rangle = \langle x_1, x_2, \ldots, x_n \rangle$ e si dice che G è *finitamente generato.*

Lemma 5.31. *Sia $X = \{x\}$. Allora il sottogruppo generato da X coincide con l'insieme $\{x^n : n \in \mathbb{Z}\}$ di tutte le potenze di x.*

DIMOSTRAZIONE. Poiché $\langle x \rangle$ è un sottogruppo, applicando (S1) e (S2) della definizione 5.23, $1 \in \langle x \rangle$ e per induzione $x^n \in \langle x \rangle$ per ogni $n \in \mathbb{N}$. Applicando (S1) e (S2) della definizione 5.23 a $x^{-1} \in \langle x \rangle$, si ottiene anche $x^n \in \langle x \rangle$ per ogni $n \in \mathbb{Z}$. Pertanto l'insieme delle potenze $H = \{x^n : n \in \mathbb{Z}\}$ è contenuto in $\langle x \rangle$. Per l'altra inclusione basta vedere che H è un sottogruppo. Infatti, se $x^n, x^m \in H$, allora $x^m x^n = x^{m+n} \in H$ e $(x^n)^{-1} = x^{-n} \in H$. Allora H è un sottogruppo che contiene x e pertanto contiene $\langle x \rangle$. □

Definizione 5.32. Un gruppo che sia generato da un solo elemento si dice *ciclico*.

I gruppi ciclici sono importanti per lo studio dei gruppi, perché un gruppo arbitrario è l'unione insiemistica dei suoi sottogruppi ciclici. Osserviamo che $\mathbb{Z}$ è un gruppo ciclico essendo generato dal suo elemento 1. Vediamo ora altri esempi di sottogruppo generato da un elemento. Calcoliamo i sottogruppi di $(\mathbb{Z}, +)$ e dimostriamo che tutti i sottogruppi di $(\mathbb{Z}, +)$ sono di questo tipo.

Lemma 5.33. *Sia $n \in \mathbb{N}$. Allora:*

(a) l'insieme $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\} = \langle n \rangle$ è un sottogruppo di $\mathbb{Z}$;
(b) se H è un sottogruppo di $\mathbb{Z}$, allora esiste $n \in \mathbb{N}$ tale che $H = n\mathbb{Z}$.

DIMOSTRAZIONE. (a) Per il lemma 5.31 in notazione additiva il sottogruppo $\langle n \rangle$ è proprio $\{nz : z \in \mathbb{Z}\}$.

(b) Se $H = \{0\}$, basta prendere $n = 0$. Supponiamo ora $H \neq 0$. Allora esiste un elemento $h \in H$, $h \neq 0$. Se $h < 0$, allora $-h \in H$ e $-h > 0$. Possiamo quindi

supporre che esista $h_1 \in H$ con $h_1 > 0$. Per il principio del buon ordinamento in $\mathbb{N}$, esiste $h_0 \in H$ tale che $h_0 > 0$ e h_0 è minimale tra tutti gli elementi positivi di H. Si ha $\langle h_0 \rangle \leq H$. Sia $x \in H$. Dividendo x per h_0 con resto troviamo $q \in \mathbb{Z}$ e $0 \leq r < h_0$ tali che $x = qh_0 + r$. Poiché $qh_0 \in H$ e $x \in H$, ne deduciamo che anche $r = x - qh_0 \in H$. Essendo $r < h_0$, r non può essere positivo. Quindi $r = 0$ e pertanto $x = qh_0 \in \langle h_0 \rangle$. Questo dimostra che $H = \langle h_0 \rangle$. □

Dato un elemento x di un gruppo G, possiamo considerare l'ordine del sottogruppo generato da x e il suo ordine come elemento di G, definito in 5.4. Dimostriamo che questa duplice definizione di "ordine" non crea ambiguità, perché i numeri interi dati dalle due definizioni coincidono.

Lemma 5.34. *Sia G un gruppo e x un suo elemento. Allora* $|\langle x \rangle| = o(x)$.

DIMOSTRAZIONE. Se $o(x) = m$, per il lemma 5.5 (b), avremo $x^n = x^k$ per $n, k \in \mathbb{Z}$ se e solo se $n \equiv_m k$. Allora, per l'osservazione 3.16,

$$\{x^n : n \in \mathbb{Z}\} = \{x^0, x^1, ..., x^{m-1}\},$$

da cui concludiamo per il lemma 5.31 che

$$|\langle x \rangle| = |\{x^0, x^1, ..., x^{m-1}\}| = m.$$

Viceversa supponiamo $|\langle x \rangle| = m$: per il lemma 5.31, esistono $n_1, n_2 \in \mathbb{Z}$, con $n_1 < n_2$ tali che $x^{n_1} = x^{n_2}$. Moltiplicando a destra e a sinistra per x^{-n_1}, otteniamo $x^{n_2 - n_1} = 1$ e $n_2 - n_1 > 0$, da cui segue che $S(x) = \{n \in \mathbb{N}_+ : x^n = 1\}$ non è vuoto. Dalla definizione 5.4 sappiamo che allora $o(x) = d < \infty$. Per quanto appena dimostrato $o(x) = d$ implica $d = |\langle x \rangle| = m$.

Abbiamo dimostrato che $o(x) = m$ se e solo se $|\langle x \rangle| = m$, da cui segue

$$o(x) = \infty \quad \text{se e solo se} \quad |\langle x \rangle| = \infty.$$

□

Si osservi che l'unione di sottogruppi non è in generale un sottogruppo. Vale infatti il seguente fatto.

Lemma 5.35. *Siano H e K sottogruppi di un gruppo G. Allora $H \cup K$ è un sottogruppo di G se e solo se $H \subseteq K$ oppure $K \subseteq H$.*

DIMOSTRAZIONE. Se $H \subseteq K$ oppure $K \subseteq H$, allora $H \cup K$ è un sottogruppo poiché in tal caso $H \cup K$ coincide con K o con H rispettivamente.

Supponiamo adesso che $H \cup K$ sia un sottogruppo di G e che $H \nsubseteq K$. Allora esiste $h \in H$ con $h \notin K$. Sia $k \in K$, allora $k \in H \cup K$ e anche $h \in H \cup K$. Poiché $H \cup K$ è un sottogruppo di G, si ha $hk \in H \cup K$, ma $hk \notin K$. Infatti, se hk fosse un elemento di K, moltiplicandolo a destra per$k^{-1} \in K$ troveremmo

$$h = (hk)k^{-1} \in K,$$

assurdo. Quindi $hk \notin K$ e di conseguenza $hk \in H$. Moltiplicando a sinistra per $h^{-1} \in H$ troviamo $k = h^{-1}(hk) \in H$. □

Corollario 5.36. *Un gruppo G non può essere unione di due suoi sottogruppi propri.*

DIMOSTRAZIONE. Supponiamo per assurdo che esistano due sottogruppi propri H, K di G tali che $G = H \cup K$. Allora per il lemma 5.35 si ha $H \leq K$ oppure $K \leq H$. Supponiamo per esempio $H \leq K$. Allora $G = H \cup K = K$, in contraddizione col fatto che K è un sottogruppo proprio di G. □

Vedremo nel lemma 5.81 che un gruppo può essere unione di tre sottogruppi propri.

Il risultato del lemma 5.35 si può generalizzare.

Lemma 5.37. *Sia*

$$H_1 \subseteq H_2 \subseteq \ldots H_n \subseteq \ldots$$

una catena crescente di sottogruppi di un gruppo G. Allora

$$H = \bigcup_{j \in \mathbb{N}_+} H_j$$

è un sottogruppo di G.

DIMOSTRAZIONE. Siano $a, b \in H$, allora $a \in H_j$ e $b \in H_k$, per qualche $j, k \in \mathbb{N}$. Sia per esempio $k \geq j$, allora $a, b \in H_k$ e quindi $ab^{-1} \in H_k \subseteq H$, poiché H_k è un sottogruppo di G. □

Siano H e K sottogruppi di G; denoteremo con $\langle H, K \rangle$ il sottogruppo $\langle H \cup K \rangle$.
Denotiamo con $\mathcal{L}(G)$ l'insieme di tutti i sottogruppi del gruppo G: allora $\mathcal{L}(G)$ è un reticolo, si veda l'esercizio 5.30.

Con il simbolo HK indichiamo l'insieme dei prodotti $\{hk \mid h \in H, k \in K\}$. Chiaramente HK è contenuto in $\langle H, K \rangle$ ma in generale non coincide con $\langle H, K \rangle$. Ad esempio, se consideriamo i sottogruppi $H = \langle (12) \rangle$ e $K = \langle (13) \rangle$ di S_3, si ha che $|HK| = 4$, mentre $|\langle H, K \rangle| = 6$.

Lemma 5.38. *Siano H e K sottogruppi di un gruppo G. Allora $HK = KH$ se e solo se $\langle H, K \rangle = HK$.*

DIMOSTRAZIONE. Se $\langle H, K \rangle = HK$, allora HK è un sottogruppo di G, che contiene sia H che K e pertanto contiene anche i loro prodotti, cioè $KH \subseteq HK$. Se consideriamo gli inversi di entrambi i lati, otteniamo $HK \subseteq KH$ e pertanto $HK = KH$. Viceversa, se $HK = KH$, basterà dimostrare che HK è un sottogruppo di G. Se $h_1, h_2 \in H$ e $k_1, k_2 \in K$, allora

$$h_1 k_1 (h_2 k_2)^{-1} = h_1 (k_1 k_2^{-1} h_2^{-1}) = h_1 (h_3 k_3)$$

per qualche $h_3 \in H$, $k_3 \in K$. Pertanto $h_1 k_1 (h_2 k_2)^{-1} = (h_1 h_3) k_3 \in HK$ e quindi HK è un sottogruppo. □

Per due sottogruppi nella particolare situazione del lemma 5.38 diamo la seguente definizione.

Definizione 5.39. Siano H, K sottogruppi di un gruppo G. Se $HK = KH$ si dice che H e K *permutano* o che sono *permutabili*.

Osservazione 5.40. Siano H, K sottogruppi di un gruppo G. Se $H \leq K$, allora $HK = K = KH$. Infatti $K \leq HK$, in quanto $1 \in H$ e $k = 1k \in HK$, per ogni $k \in K$. Inoltre $HK \leq K$, in quanto $h \in H \leq K$, implica $hk \in K$.

È noto che vale la legge distributiva dell'unione rispetto all'intersezione di insiemi. Vediamo che in generale la legge distributiva del prodotto di sottogruppi rispetto all'intersezione non vale, cioè dati tre qualsiasi sottogruppi H, K, L di un gruppo G, *non* vale $(HK) \cap L = (H \cap L)(K \cap L)$. Osserviamo che una delle due inclusioni è vera.

Osservazione 5.41. Dati H, K, L sottogruppi di un gruppo G si ha

$$(H \cap L)(K \cap L) \subseteq (HK) \cap L.$$

Infatti

$$H \cap L \subseteq H \;\text{ e }\; K \cap L \subseteq K \implies (H \cap L)(K \cap L) \subseteq HK,$$

ma anche

$$H \cap L \subseteq L \;\text{ e }\; K \cap L \subseteq L \implies (H \cap L)(K \cap L) \subseteq L,$$

in quanto L è un sottogruppo.

Il seguente esempio dimostra che l'altra inclusione non vale in generale, si veda anche l'esercizio 5.29 per un esempio con un gruppo abeliano infinito.

Esempio 5.42. Siano $G = S_3$, $H = \langle(123)\rangle$, $K = \langle(12)\rangle$ e $L = \langle(13)\rangle$. Allora $HK = G$, $H \cap L = \{1\}$ e $K \cap L = \{1\}$ da cui

$$(HK) \cap L = G \cap L = L = \langle(13)\rangle > (H \cap L)(K \cap L) = \{1\}.$$

Vale però una forma particolare della legge distributiva.

Teorema 5.43. (Legge modulare di Dedekind) *Siano H, K, L sottogruppi di un gruppo G e sia $K \subseteq L$. Allora*

$$(HK) \cap L = (H \cap L)K.$$

In particolare, se H e K permutano, si ha

$$\langle H, K\rangle \cap L = \langle H \cap L, K\rangle.$$

DIMOSTRAZIONE. La prima inclusione è già stata dimostrata nel caso più generale nell'osservazione 5.41. Viceversa supponiamo $x \in (HK) \cap L$; allora $x = hk$ per qualche $h \in H$ e $k \in K$, da cui $h = xk^{-1} \in LK = L$, cioè $h \in H \cap L$ e dunque $x \in (H \cap L)K$. La seconda parte discende direttamente dal lemma 5.38. □

5.4 Classi laterali di un sottogruppo

Se H è un sottogruppo di un gruppo G, introduciamo in G una relazione binaria ponendo $x \sim y$ quando $x^{-1}y \in H$.

Lemma 5.44. *Siano G un gruppo, H un sottogruppo di G, $x, y \in G$ e*

$$x \sim y \iff x^{-1}y \in H.$$

Allora:

(a) $\sim$ è una relazione di equivalenza;
(b) la classe di equivalenza $[x]_\sim$ coincide con l'insieme $\{xh : h \in H\}$, che denoteremo brevemente con xH;
(c) $\{xH : x \in G\}$ è una partizione di G.

DIMOSTRAZIONE. (a) Sia $x \in G$. Allora $x \sim x$ in quanto $x^{-1}x \in H$. Se $x \sim y$, allora $x^{-1}y \in H$. Per la proprietà (S2) della definizione 5.23 ricaviamo

$$y^{-1}x = (x^{-1}y)^{-1} \in H$$

e di conseguenza $y \sim x$. Se $x \sim y$ e $y \sim z$, allora $x^{-1}y \in H$ e $y^{-1}z \in H$. Moltiplicando questi due elementi di H si ricava da (S1)

$$x^{-1}z = (x^{-1}y)(y^{-1}z) \in H.$$

(b) Sia $y \in [x]_\sim$. Allora $x \sim y$ e quindi $x^{-1}y \in H$. Pertanto $x^{-1}y = h$ per qualche elemento $h \in H$. Deduciamo che $y = xh$.

Viceversa, se $y = xh$ per qualche elemento $h \in H$, allora $x^{-1}y = h \in H$ e quindi $x \sim y$ e $y \in [x]_\sim$.

(c) Le classi di equivalenza di una relazione di equivalenza costituiscono una partizione, quindi per (a) e (b) $\{xH : x \in G\}$ è una partizione di G. □

In seguito chiameremo la classe di equivalenza xH *classe laterale sinistra* di H in G.

Dato un sottogruppo H del gruppo G, si introduce un'altra relazione $\sim'$ per $x, y \in G$ ponendo $x \sim' y$ se e solo se $xy^{-1} \in H$. Si dimostra in modo analogo al precedente il seguente lemma.

Lemma 5.45. *Siano G un gruppo, H un sottogruppo di G, $x, y \in G$ e*

$$x \sim' y \iff xy^{-1} \in H.$$

Allora:

(a) $\sim'$ è una relazione di equivalenza;
(b) la classe di equivalenza $[x]_{\sim'}$ coincide con l'insieme $\{hx : h \in H\} = Hx$;
(c) $\{Hx\}_{x \in G}$ è una partizione di G.

La classe di equivalenza Hx si dice *classe laterale destra* di H in G.

Osserviamo che se G è un gruppo abeliano, H un suo sottogruppo e $x \in G$, allora la classe laterale sinistra in notazione additiva è $x + H$ che coincide con la classe laterale destra $H + x$, visto che ogni elemento di H commuta con x.

La seguente facile osservazione verrà utilizzata numerose volte.

Osservazione 5.46. Sia H un sottogruppo di un gruppo G e $x, y \in G$. Allora

$$xH = yH \iff x^{-1}y \in H \iff x \in yH, \quad \text{e}$$

$$Hx = Hy \iff xy^{-1} \in H \iff x \in Hy.$$

Vediamo alcuni esempi.

Esempio 5.47. Sia $G = (\mathbb{Z}, +)$ e sia $H = 4\mathbb{Z}$. Abbiamo visto nel lemma 5.33 che H è un sottogruppo di G. Troviamo le classi laterali sinistre (e quindi destre) di H:

$$0 + 4\mathbb{Z} = \{4m : m \in \mathbb{Z}\}, \qquad 1 + 4\mathbb{Z} = \{1 + 4m : m \in \mathbb{Z}\},$$

$$2 + 4\mathbb{Z} = \{2 + 4m : m \in \mathbb{Z}\}, \qquad 3 + 4\mathbb{Z} = \{3 + 4m : m \in \mathbb{Z}\}.$$

Vediamo ora un esempio di un sottogruppo di un gruppo finito non abeliano in cui le classi laterali sinistre non coincidono con le classi laterali destre.

Esempio 5.48. Sia $G = S_3$ il gruppo delle permutazioni su 3 oggetti e sia $H = \langle(12)\rangle$. Troviamo le classi laterali sinistre di H:

$id \circ H = \{id, (12)\}$,
$(123) \circ H = \{(123), (13)\}$,
$(132) \circ H = \{(132), (23)\}$.

Mentre le classi laterali destre sono:

$H \circ id = \{id, (12)\}$,
$H \circ (123) = \{(123), (23)\}$,
$H \circ (132) = \{(132), (13)\}$.

In generale quindi le classi laterali destre e sinistre non coincidono. Si può invece dimostrare che hanno la stessa cardinalità.

Lemma 5.49. *Sia G un gruppo ed $H \leq G$. Ogni classe laterale di H in G ha la stessa cardinalità di H.*

DIMOSTRAZIONE. Sia $x \in G$. Definiamo un'applicazione $f : H \to xH$ ponendo $f(h) = xh$. Per la definizione di xH, f è suriettiva. Verifichiamo che f è iniettiva. Infatti, se $f(h) = f(h')$, allora $xh = xh'$ e per la legge di cancellazione si ottiene $h = h'$. Quindi xH ha la stessa cardinalità di H. Allo stesso modo si verifica che le classi laterali destre hanno la stessa cardinalità di H. □

Lemma 5.50. *Sia G un gruppo ed $H \leq G$. La cardinalità dell'insieme $\{xH\}_{x \in G}$ delle classi laterali sinistre di H in G coincide con la cardinalità dell'insieme $\{Hx\}_{x \in G}$ delle classi laterali destre di H in G.*

DIMOSTRAZIONE. Ad ogni classe laterale sinistra xH corrisponde la classe laterale destra Hx^{-1} e questa corrispondenza definisce una biezione tra i due insiemi. □

Definizione 5.51. La cardinalità comune degli insiemi $\{xH\}_{x\in G}$ e $\{Hx\}_{x\in G}$ si indica con $[G:H]$ e si dice *indice* del sottogruppo H in G.

Il seguente celebre teorema di Lagrange rivela una relazione semplice, ma molto utile tra la cardinalità di un sottogruppo H di un gruppo finito G e l'indice di H in G.

Teorema 5.52. (Teorema di Lagrange) *Siano G un gruppo finito ed H un suo sottogruppo. Allora*

$$|G| = [G:H]|H|.$$

DIMOSTRAZIONE. Abbiamo dimostrato che la relazione $\sim$ definita nel lemma 5.44 è una relazione di equivalenza. Pertanto G è unione disgiunta delle classi di equivalenza, cioè di classi laterali sinistre di H in G. Ci sono esattamente $[G:H]$ di queste classi e dal lemma 5.49 ognuna di queste ha la stessa cardinalità di H. Allora $|G| = [G:H]|H|$. □

Il teorema di Lagrange ha un importantissimo corollario che consente di mettere in relazione l'ordine di un gruppo finito e quello dei suoi sottogruppi.

Corollario 5.53. *Sia G un gruppo finito e H un sottogruppo di G. Allora $|H|$ e $[G:H]$ dividono $|G|$.*

Quindi se consideriamo un gruppo di ordine 12, come ad esempio $G = \mathbb{Z}_{12}$, G non potrà avere sottogruppi di ordine 5 o 10, ma potrà avere sottogruppi di ordine $2, 3, 4$ o 6, oltre a quelli banali di ordine 1 e 12. Analogamente se consideriamo il gruppo A_4, anch'esso di ordine 12, esso può avere sottogruppi di ordine $1, 2, 3, 4, 6, 12$, ma come vedremo nell'esempio 8.21, non è detto che li abbia.

Il teorema di Lagrange permette di conoscere i possibili periodi degli elementi di un certo gruppo finito G.

Corollario 5.54. *Sia G un gruppo finito e x un elemento di G. Allora $o(x)$ divide $|G|$ e $x^{|G|} = 1$.*

DIMOSTRAZIONE. Per il lemma 5.34 $o(x) = |\langle x\rangle|$. Allora dal corollario 5.53 segue che $o(x)$ divide $|G|$. Inoltre $x^{|G|} = 1$ per il lemma 5.5 (a). □

Un caso particolare si ha quando tutti gli elementi di un gruppo G hanno ordine una potenza di uno stesso primo p.

Definizione 5.55. Sia p un primo fissato. Un gruppo G in cui ogni elemento ha ordine p^n, per qualche $n \in \mathbb{N}$, si dice *p-gruppo*. Un p-sottogruppo di un gruppo G è un sottogruppo di G che è un p-gruppo.

Il corollario 5.54 garantisce che se un gruppo G ha ordine p^n, allora tutti i suoi elementi hanno ordine che divide p^n e pertanto G è un p-gruppo. Nel lemma 8.13 dimostreremo che se p è un primo, i p-gruppi finiti sono esattamente i gruppi di ordine p^n, per qualche $n \in \mathbb{N}_+$.

C'è un importante teorema della teoria dei gruppi finiti che permette di invertire parzialmente il teorema di Lagrange in un caso particolare.

Il primo teorema di Sylow 8.17 che dimostreremo nel capitolo 8 afferma che se G è un gruppo finito di ordine divisibile per il primo p e p^a è la massima potenza di p che divide l'ordine di G, allora esiste un sottogruppo di ordine esattamente p^a.

Definizione 5.56. Sia G gruppo finito, $|G| = p^a n$, con p primo e $(p, n) = 1$. Allora un sottogruppo P di G di ordine p^a si dice un *p-sottogruppo di Sylow di G*. L'insieme dei p-sottogruppi di Sylow di G si denota con $Syl_p(G)$.

Abbiamo visto che c'è una relazione tra l'ordine di un gruppo G e l'ordine dei suoi elementi. Se l'insieme $\{n \in \mathbb{N}_+ : x^n = 1 \ \forall x \in G\}$ non è vuoto, il minimo di tale insieme si dice l'*esponente* di G e si denota con $\exp(G)$.

Esempio 5.57. L'esponente del gruppo $\mathbb{Z}_8$ è 8, mentre $\exp(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$. Infine $\exp(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$. Nell'esercizio 7.30, si chiede di dimostrare che se G è un gruppo abeliano, allora $|G| = \exp(G)$ se e solo se G è ciclico. Questa proprietà non è vera nei gruppi non abeliani, in quanto $\exp(S_3) = 6 = |S_3|$, ma S_3 non è ciclico.

Osservazione 5.58. Osserviamo che se G è finito, allora

$$\exp(G) = m.c.m.\{o(x) : x \in G\}.$$

Pertanto se G è un gruppo finito di ordine n, allora $\exp(G)$ divide n. Infatti se $x \in G$, si ha che $o(x)$ divide $|G|$ per il corollario 5.54, da cui segue l'asserto.

Applichiamo il teorema di Lagrange per determinare tutti i sottogruppi di alcuni gruppi.

Esempio 5.59. Calcoliamo tutti i sottogruppi di $G = (\mathbb{Z}_3, +)$. Se H è un sottogruppo di G, $|H|$ deve dividere 3. Quindi le sole possibilità sono $|H| = 1, 3$, da cui segue che H può essere solo $\{0\}$ o G.

Come si vede dall'esempio 5.59, lo stesso ragionamento vale ogni qualvolta si abbia un gruppo di ordine un numero primo. Inoltre i gruppi di ordine un primo sono sempre ciclici.

Lemma 5.60. *Sia G un gruppo di ordine p, con p primo. Allora:*

(a) gli unici sottogruppi di G sono $\{1_G\}$ e G;
(b) G è ciclico;
(c) tutti gli elementi non nulli di G hanno ordine p e generano G.

DIMOSTRAZIONE. (a) Se H è un sottogruppo di G, $|H|$ deve dividere p per il corollario 5.53. Quindi le sole possibilità sono $|H| = 1$ o p, da cui segue che H può essere solo $\{1_G\}$ o G.

(b) - (c) Sia x un elemento di G, $x \neq 1$. Allora $|\langle x \rangle| = p$ per (a) e quindi $\langle x \rangle$ coincide con G. Per il lemma 5.34 si ha infine $o(x) = p$. □

Il teorema di Lagrange vale solo per gruppi finiti. Si può dire qualcosa anche per i gruppi infiniti, come si dimostra nel seguente lemma.

Lemma 5.61. *Se H e K sono sottogruppi di indice finito del gruppo G, allora anche il sottogruppo $H \cap K$ ha indice finito in G.*

DIMOSTRAZIONE. Basta provare che il sottogruppo $H \cap K$ ha un numero finito di classi laterali sinistre. Le classi laterali sinistre di $H \cap K$ sono le classi di equivalenza della relazione di equivalenza $\sim$ definita da $x \sim y$ se e solo se $x^{-1}y \in H \cap K$. Questo è equivalente a $x^{-1}y \in H$ e $x^{-1}y \in K$, cioè $x \sim_H y$ e $x \sim_K y$, dove $\sim_H$ e $\sim_K$ sono le relazioni di equivalenza relative ai sottogruppi H e K. Queste ultime relazioni di equivalenza danno luogo alle partizioni $G = \bigcup_{x \in G} xH$ e $G = \bigcup_{x \in G} xK$ di G che sono finite per ipotesi. Le classi di equivalenza della relazione $\sim$ sono intersezioni delle classi di equivalenza delle relazioni $\sim_H$ e $\sim_K$. Pertanto tutte le intersezioni non vuote $\{xH \cap yK\}_{x,y \in G}$ sono un numero finito e danno luogo ad una partizione nuova che corrisponde alla relazione di equivalenza $\sim$. □

In generale, se G è un gruppo infinito e H un sottogruppo di G, si ha

$$|G| = \max\{[G : H], |H|\}.$$

La dimostrazione di questo fatto, che utilizza proprietà dei numeri cardinali infiniti, viene lasciata nell'esercizio 5.23.

5.5 Sottogruppi normali

Definizione 5.62. Un sottogruppo H di un gruppo G si dice *normale* se vale

$$xH = Hx \quad \text{per ogni elemento} \quad x \in G.$$

Si denota brevemente con $H \trianglelefteq G$.

Quando un sottogruppo H di un gruppo G è normale, non c'è più distinzione tra classi laterali *sinistre* e classi laterali *destre*. L'insieme delle classi laterali di H in G si indica con G/H.

Lemma 5.63. *Se G è un gruppo abeliano, allora tutti i sottogruppi di G sono normali.*

DIMOSTRAZIONE. Se G è abeliano e H è un sottogruppo di G, allora $xh = hx$ per ogni $x \in G$, $h \in H$ e quindi $xH = Hx$ per ogni $x \in G$, cioè H è normale. □

Non è però vero il viceversa. Esistono cioè dei gruppi non abeliani in cui tutti i sottogruppi sono normali, come vedremo nel lemma 5.81.

Se il gruppo non è abeliano, non è detto che tutti i sottogruppi siano normali, come abbiamo verificato nell'esempio 5.48: se $G = S_3$ e $H = \langle(12)\rangle$, allora la classe laterale sinistra $(123) \circ H$ non coincide con la classe laterale destra $H \circ (123)$.

Dimostriamo ora un utile criterio per verificare se un sottogruppo di un gruppo G è normale, senza dover controllare l'uguaglianza delle classi laterali destre e sinistre.

Lemma 5.64. *Un sottogruppo H di un gruppo G è normale se e solo se*

$$x^{-1}hx \in H \text{ per ogni } x \in G \text{ e per ogni } h \in H. \tag{3}$$

DIMOSTRAZIONE. Supponiamo che H sia normale. Sia $x \in G$ e $h \in H$. Allora $hx \in Hx = xH$, quindi esiste $h' \in H$ tale che $hx = xh'$. Di conseguenza

$$x^{-1}hx = h' \in H.$$

Questo dimostra (3).

Supponiamo ora che valga (3). Per dimostrare che H è normale bisogna provare che $xH = Hx$ per ogni elemento $x \in G$. Sia $x \in G$ e $xh \in xH$: per (3) applicata all'elemento x^{-1}, esiste un elemento $h' \in H$ tale che $xhx^{-1} = h'$. Allora $xh = h'x$ e quindi $xh \in Hx$. Per dimostrare l'inclusione $Hx \subseteq xH$ si prenda un elemento $hx \in Hx$. Per (3) abbiamo $x^{-1}hx \in H$ e quindi $x^{-1}hx = h'$ per qualche $h' \in H$. Di conseguenza $hx = xh' \in xH$. □

Osservazione 5.65. Nella dimostrazione precedente abbiamo sfruttato il fatto che (3) significa $x^{-1}hx = h'$ per *ogni elemento* $x \in G$, *ogni elemento* $h \in H$ *e un opportuno elemento* $h' \in H$. In generale h' può non coincidere con h. Tuttavia questa regola di *scambio* permette di avere per ogni $x \in G$ e per ogni $h \in H$ un elemento $h' \in H$ tale che $hx = xh'$.

Definizione 5.66. Sia G un gruppo e $x \in G$. Allora il *coniugato* di x tramite $g \in G$ è l'elemento $g^{-1}xg$, che denotiamo con x^g. Se H è un sottogruppo di G, il *coniugato* di H tramite g è il sottoinsieme $\{h^g : h \in H\}$, che denotiamo con H^g.

In questi termini nell'osservazione 5.65 h' è il coniugato di h tramite x. È facile verificare che H^g è un sottogruppo di G, si veda l'esercizio 5.31.

Usando il lemma 5.64 e la notazione appena introdotta si dimostra il seguente lemma.

Lemma 5.67. *Sia N un sottogruppo di G. Allora sono equivalenti:*

(a) N è normale in G;
(b) $N^g \leq N$ per ogni $g \in G$;
(c) $N = N^g$ per ogni $g \in G$.

DIMOSTRAZIONE. (a) è equivalente a (b) per il lemma 5.64.

È sufficiente verificare che (b) implica (c), essendo l'altra implicazione ovvia. Sia $g \in G$, allora per (b) applicata a g^{-1} si ha $N^{g^{-1}} \leq N$, cioè $gNg^{-1} \leq N$, da cui si ottiene, moltiplicando a destra per g e a sinistra per g^{-1}, $N \leq g^{-1}Ng$, che conclude la dimostrazione. □

Lemma 5.68. *Se H è un sottogruppo di un gruppo G e K è un sottogruppo normale di G allora $HK = KH$. In particolare HK è un sottogruppo di G. Se anche H è normale, allora HK è un sottogruppo normale di G.*

DIMOSTRAZIONE. Poiché K è normale, $hK = Kh$ per ogni $h \in H$ e quindi

$$HK = \bigcup_{h\in H} hK = \bigcup_{h\in H} Kh = KH.$$

Inoltre per il lemma 5.38, KH è un sottogruppo.

Usiamo il lemma 5.64 per dimostrare che HK è normale se H e K lo sono. Sia $x \in G$ e $hk \in HK$, cioè $h \in H$ e $k \in K$. Allora

$$x^{-1}hkx = x^{-1}h(xx^{-1})kx = (x^{-1}hx)(x^{-1}kx) \in HK,$$

in quanto $x^{-1}hx \in H$ e $x^{-1}kx \in K$ perché H e K sono normali. □

Abbiamo visto che l'intersezione di sottogruppi è ancora un sottogruppo. Lo stesso vale anche per i sottogruppi normali.

Lemma 5.69. *Sia $\{N_i : i \in I\}$ una famiglia di sottogruppi normali di un gruppo G. Allora:*

(a) $\bigcap_{i\in I} N_i$ è un sottogruppo normale di G;
(b) $\langle N_i : i \in I\rangle$ è un sottogruppo normale di G.

DIMOSTRAZIONE. (a) Sia $x \in \bigcap_{i\in I} N_i$, allora $x \in N_i$, per ogni $i \in I$ e per il lemma 5.67 si ha $x^g \in N_i$, per ogni $i \in I$ e per ogni $g \in G$. Quindi $x^g \in \bigcap_{i\in I} N_i$ e dunque

$$\left(\bigcap_{i\in I} N_i\right)^g \leq \bigcap_{i\in I} N_i,$$

che permette di concludere grazie al lemma 5.67.

(b) Sia $x \in \langle N_i : i \in I\rangle$. Per il lemma 5.68 si ha $x = x_1x_2\ldots x_r$ con $x_j \in N_{i_j}$ per qualche $i_1, \ldots, i_r \in I$. Quindi

$$x^g = g^{-1}xg = (g^{-1}x_1g)(g^{-1}x_2g)\ldots(g^{-1}x_rg) \in \langle N_i : i \in I\rangle$$

per il lemma 5.67, visto che N_{i_j} è normale per ogni $j = 1, \ldots, r$. Abbiamo dimostrato che

$$\langle N_i : i \in I\rangle^g \leq \langle N_i : i \in I\rangle$$

e quindi concludiamo per il lemma 5.67. □

Per il lemma 5.69 l'insieme di tutti i sottogruppi normali di un gruppo G, che denoteremo con $\mathcal{N}(G)$ è un reticolo. Osserviamo che $\{1\}$ e G sono normali in G.

Potrebbe accadere che il reticolo dei sottogruppi normali $\mathcal{N}(G)$ contenga solo i sottogruppi banali $\{1\}$ e G.

Definizione 5.70. Un gruppo privo di sottogruppi normali non banali si dice *semplice*.

Abbiamo già osservato nel lemma 5.60 che un gruppo di ordine un primo p non ha sottogruppi non banali, quindi a maggior ragione non ha sottogruppi normali non banali. Pertanto i gruppi $(\mathbb{Z}_p, +)$ sono gruppi semplici. Si può dimostrare anzi che sono i soli gruppi abeliani semplici. Ci sono anche gruppi semplici non abeliani, che hanno invece "molti" sottogruppi non normali. Un'intera famiglia di gruppi semplici non abeliani è data dai gruppi alterni A_n, come dimostreremo più avanti nel teorema 8.27. Un esempio di gruppo semplice infinito viene descritto nell'esercizio 8.4.

Per ogni gruppo G possiamo definire un sottogruppo che è senz'altro normale, ma potrebbe essere banale: un sottogruppo che "misura" quanti elementi commutano con tutti gli elementi del gruppo.

Definizione 5.71. Un elemento $z \in G$ si dice *centrale* in G se $zg = gz$ per ogni $g \in G$. L'insieme degli elementi centrali

$$Z(G) = \{z \in G \mid zg = gz \text{ per ogni} g \in G\}$$

si chiama *centro* di G.

Lemma 5.72. *Il centro di un gruppo G è un sottogruppo abeliano normale di G. Ogni sottogruppo contenuto nel centro di G è normale in G.*

DIMOSTRAZIONE. Sia $Z(G)$ il centro di G, allora $1 \in Z(G)$. Siano $z, w \in Z(G)$ e $x \in G$. Dimostriamo che z^{-1}, zw e $x^{-1}zx$ appartengono a $Z(G)$. Sia $g \in G$; dal fatto che $z \in Z(G)$ segue che $zg = gz$, da cui, moltiplicando per z^{-1} a destra e a sinistra, ricaviamo $gz^{-1} = z^{-1}g$, cioè $z^{-1} \in Z(G)$. Inoltre

$$(zw)g = z(wg) = z(gw) = (zg)w = g(zw),$$

cioè anche $zw \in Z(G)$.

Dalla definizione segue che $zw = wz$ e quindi $Z(G)$ è abeliano. Infine

$$x^{-1}zx = x^{-1}(zx) = x^{-1}(xz) = (x^{-1}x)z = z \in Z(G),$$

da cui segue che $Z(G)$ è normale per il lemma 5.64.

La stessa dimostrazione prova che ogni sottogruppo contenuto nel centro di G è normale in G. □

Osserviamo che, come accennato prima, G è abeliano se e solo se $Z(G) = G$, mentre se G è un gruppo semplice non abeliano il centro di G è banale (si veda l'esercizio 5.32).

5.6 Gruppi lineari

In questo paragrafo vogliamo studiare i *gruppi lineari*, cioè insiemi di applicazioni lineari invertibili su uno spazio vettoriale di dimensione finita che sono gruppi con l'operazione di composizione di applicazioni. È chiaro proprio dalla loro definizione che i gruppi lineari costituiscono un legame importante tra la geometria e l'algebra.

Avevamo introdotto nella definizione 4.30 il gruppo generale lineare $GL_n(K)$ di dimensione n su un campo K.

Definizione 5.73. Una matrice $(a_{ij}) \in GL_n(K)$ tale che $a_{ij} = 0$ se $i \neq j$, $a_{ii} = a_{jj}$ per $i, j = 1, \ldots, n$ si dice una *matrice scalare*.

Si vede facilmente che le matrici scalari formano un sottogruppo di $GL_n(K)$. Introduciamo ora altri sottogruppi di $GL_n(K)$.

Lemma 5.74. *Siano $n > 1$ un intero e K un campo. Allora:*

(a) il sottoinsieme $SL_n(K)$ del gruppo lineare $GL_n(K)$ formato dalle matrici con determinante uguale a 1 è un sottogruppo normale;
(b) il sottoinsieme $\mathrm{T}_n^+(K) = \{(a_{ij}) \in GL_n(K) : a_{ij} = 0$ se $i > j\}$ di $GL_n(K)$ formato delle matrici triangolari superiori è un sottogruppo di $GL_n(K)$; $\mathrm{T}_n^+(K)$ non è normale;
(c) il sottoinsieme $\mathrm{D}_n(K) = \{(a_{ij}) \in GL_n(K) : a_{ij} = 0$ se $i \neq j\}$ di $GL_n(K)$ formato delle matrici diagonali è un sottogruppo di $GL_n(K)$; $\mathrm{D}_n(K)$ non è normale, se $|K| \geq 3$;
(d) il centro di $GL_n(K)$ è l'insieme delle matrici scalari Z.

DIMOSTRAZIONE. (a) Innanzitutto $SL_n(K)$ non è vuoto, perché la matrice identica $I_n \in SL_n(K)$. Inoltre, se $A, B \in SL_n(K)$, si ha $\det(A) = \det(B) = 1$ da cui, per il teorema di Binet 4.31 e per il corollario 4.32 (a),

$$\det(A^{-1}B) = \det(A^{-1})\det(B) = \det(A)^{-1}\det(B) = 1.$$

Quindi $SL_n(K)$ è un sottogruppo. Dimostriamo che è normale. Se $C \in GL_n(K)$, allora

$$\det(C^{-1}AC) = \det(A) = 1$$

per il corollario 4.32 (b), da cui segue che $SL_n(K)$ è normale.

(b) Innanzitutto $\mathrm{T}_n^+(K)$ non è vuoto, perché la matrice identica $I_n \in \mathrm{T}_n^+(K)$. Siano $A, B \in \mathrm{T}_n^+(K)$. Utilizzando la definizione dell'inversa di A, si può provare che anche $A^{-1} \in \mathrm{T}_n^+(K)$. Inoltre se $AB = C = (c_{ij})$ e $i > j$ si ha

$$c_{ij} = \sum_{l=1}^{n} a_{il}b_{lj},$$

ove se $i > l$, $a_{il} = 0$ e se $i \leq l$, allora $j < i \leq l$, da cui $b_{lj} = 0$. Pertanto $c_{ij} = 0$ per ogni $i, j = 1, \ldots, n$ e $i > j$, cioè $AB = C \in \mathrm{T}_n^+(K)$.

Per dimostrare che non è un sottogruppo normale, lo dimostriamo dapprima nel caso $n = 2$, prendendo la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{T}_n^+(K)$ e la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_n(K)$:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

che non appartiene a $\mathrm{T}_n^+(K)$. Il caso $n > 2$ si ottiene allo stesso modo, completando opportunamente le matrici utilizzate nel caso $n = 2$.

(c) L'insieme $\mathrm{D}_n(K)$ non è vuoto, perché la matrice identica $I_n \in \mathrm{D}_n(K)$. Siano $A = (a_{ii}), B = (b_{ii}) \in \mathrm{D}_n(K)$. Utilizzando la definizione dell'inversa di A, si può provare che $A^{-1} = (a_{ii}^{-1}) \in \mathrm{D}_n(K)$. Inoltre se $C = AB = (c_{ij})$, una semplice verifica prova che $c_{ij} = 0$ se $i \neq j$ e $c_{ii} = a_{ii}b_{ii}$ per ogni $i, j = 1, ..., n$.

Supponiamo $|K| \geq 3$, allora esistono due elementi distinti non nulli $a \neq b$. Supponiamo $n = 2$ e consideriamo le matrici

$$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in \mathrm{D}_n(K) \text{ e } B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_n(K):$$

$$B^{-1}AB = \begin{pmatrix} a & 0 \\ a-b & b \end{pmatrix} \notin \mathrm{D}_n(K) \quad \text{perché} \quad a - b \neq 0.$$

Il caso $n > 2$ si ottiene allo stesso modo, completando opportunamente le matrici utilizzate nel caso $n = 2$.

(d) Siano $A, B \in Z$ e $C \in GL_n(K)$. Allora $A = aI_n$, $B = bI_n$, per qualche $a, b \in K \setminus \{0\}$ e vale

$$AB = abI_n, \quad A^{-1} = a^{-1}I_n, \quad AC = aC = Ca = CA.$$

Questo prova che Z è un sottogruppo contenuto nel centro di $GL_n(K)$.

Sia $A = (a_{ij}) \in Z(GL_n(K))$ e siano E_{rs} le matrici definite nell'esempio 4.23. Definiamo $B_{rs} = I_n + E_{rs}$ e osserviamo che $\det(B_{rs}) = 1$, se $r \neq s$. Quindi $B_{rs} \in GL_n(K)$ per ogni $r, s = 1, \ldots n$, $r \neq s$. Fissiamo B_{rs}; poiché A commuta con B_{rs}, si ha

$$AB_{rs} = A(I_n + E_{rs}) = A + AE_{rs} = B_{rs}A = (I_n + E_{rs})A = A + E_{rs}A,$$

da cui si ottiene $AE_{rs} = E_{rs}A$. Ora la matrice AE_{rs} ha tutti gli elementi nulli eccetto nella colonna s, data dal vettore colonna $(a_{1r}, \ldots, a_{nr})$. La matrice $E_{rs}A$ ha invece tutte le righe nulle eccetto l'r-esima riga, data dal vettore $(a_{s1}, \ldots, a_{sn})$. Uguagliando queste due matrici, concludiamo che $a_{ir} = 0$ per ogni $i \neq r$ e che $a_{rr} = a_{ss}$.

Dal fatto che A commuta con B_{rs} per ogni $r, s = 1, \ldots n$, $r \neq s$, segue che $a_{ir} = 0$ per ogni $i, r = 1, \ldots n$, $i \neq r$ e $a_{rr} = a_{ss}$ per ogni $r, s = 1, \ldots n$, cioè $A \in Z$. □

Osservazione 5.75. Il gruppo $GL_n(K)$ è un gruppo non abeliano per qualsiasi campo K e per $n \geq 2$, per il punto (d) del lemma 5.74.

In modo del tutto analogo si dimostra che anche il sottoinsieme delle matrici triangolari inferiori $\mathrm{T}_n^-(K) = \{(a_{ij}) \in GL_n(K) : a_{ij} = 0 \text{ se } i < j\}$ è un sottogruppo di $GL_n(K)$. Allora vale il seguente facile lemma.

Lemma 5.76. *L'intersezione del sottogruppo delle matrici triangolari superiori con il sottogruppo delle matrici triangolari inferiori è il sottogruppo delle matrici diagonali, cioè*

$$\mathrm{T}_n^+(K) \cap \mathrm{T}_n^-(K) = \mathrm{D}_n(K).$$

DIMOSTRAZIONE. Sia $A = (a_{ij}) \in \mathrm{T}_n^+(K) \cap \mathrm{T}_n^-(K)$; allora $a_{ij} = 0$ per ogni $i < j$ e $j < i$, $i, j = 1, 2, \ldots, n$, da cui $a_{ij} = 0$ per ogni $i \neq j$, $i, j = 1, 2, \ldots, n$, cioè $A = (a_{ij}) \in \mathrm{D}_n(K)$. L'altra inclusione è ovvia. □

Vogliamo ora introdurre un altro gruppo lineare, cioè un sottogruppo di $GL_n(K)$. Per far questo abbiamo bisogno della seguente definizione.

Definizione 5.77. Sia $A = (a_{ij}) \in M_{m\times n}(K)$; definiamo la *matrice trasposta* di A come la matrice $B = (b_{ij})$ con $b_{ij} = a_{ji}$. Denotiamo la matrice trasposta di A con $A^t = (a_{ji})$.

Si prova facilmente che per $A, B \in \mathrm{M}_n(K)$, si ha $(AB)^t = B^t A^t$, si veda l'esercizio 5.34. Ci si può chiedere quando una matrice $A \in \mathrm{M}_n(K)$ coincide con la sua trasposta. Le matrici di questo tipo hanno un nome.

Definizione 5.78. Una matrice $A \in \mathrm{M}_n(K)$ tale che $A^t = A$ si dice *simmetrica* .

L'insieme di tutte le matrici simmetriche di $GL_n(K)$ non forma un sottogruppo di $GL_n(K)$, come si chiede di dimostrare nell'esercizio 5.44. Consideriamo il sottoinsieme di tutte le matrici di $GL_n(K)$ tali che l'inversa coincide con la trasposta. Dimostriamo nel seguente lemma che questo insieme è un sottogruppo di $GL_n(K)$.

Lemma 5.79. *(a) Se $A \in GL_n(K)$, allora $(A^t)^{-1} = (A^{-1})^t$.*
(b) Sia $\mathrm{O}_n(K) = \{A \in GL_n(K) : A^{-1} = A^t\}$. Allora $\mathrm{O}_n(K)$ è un sottogruppo di $GL_n(K)$.

DIMOSTRAZIONE. (a) Sia $A \in GL_n(K)$ e I_n la matrice identica di $GL_n(K)$. Allora

$$I_n = (I_n)^t = (AA^{-1})^t = (A^{-1})^t A^t$$

da cui segue che l'inversa di A^t, cioè $(A^t)^{-1}$ è proprio $(A^{-1})^t$.

(b) L'insieme $\mathrm{O}_n(K)$ non è vuoto perché la matrice identica $I_n \in \mathrm{O}_n(K)$. Inoltre se $A, B \in \mathrm{O}_n(K)$, per (a) e per la definizione di $\mathrm{O}_n(K)$ si ha

$$(A^{-1})^t = (A^t)^{-1} = (A^{-1})^{-1} = A,$$

cioè $A^{-1} \in \mathrm{O}_n(K)$. Inoltre

$$(AB)^{-1} = B^{-1}A^{-1} = B^t A^t = (AB)^t,$$

da cui segue che $AB \in \mathrm{O}_n(K)$. □

I sottogruppi definiti nei lemmi 5.74 e 5.79 hanno i seguenti nomi.

Definizione 5.80. Il gruppo $SL_n(K)$ si chiama *gruppo speciale lineare*, il gruppo $O_n(K)$ si chiama *gruppo ortogonale lineare.*

I gruppi lineari fino ad ora considerati possono essere definiti su qualsiasi campo. Infatti nelle definizioni non abbiamo introdotto nessuna ipotesi sul campo K. Passiamo ora a considerare alcuni casi particolari, specializzando lo studio per esempio al campo dei complessi o ai campi finiti.

Cominciamo con il gruppo Q_8 dei *quaternioni* di ordine 8. Lo definiamo come sottogruppo del gruppo lineare $GL_2(\mathbb{C})$. Anche Q_8, come S_3, è il più piccolo gruppo che gode di diverse proprietà. Ad esempio è il più piccolo gruppo non abeliano di ordine una potenza di un primo, o ancora è il più piccolo gruppo non abeliano in cui tutti i sottogruppi sono normali. Infine, come dimostriamo nel seguente lemma 5.81, Q_8 è l'unione di tre suoi sottogruppi propri. È il più piccolo gruppo che gode di questa proprietà? Si veda l'esercizio 5.43.

Lemma 5.81. *Siano*

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

elementi di $GL_2(\mathbb{C})$ *e* $Q_8 = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$, *ove* 1 *denota la matrice identica* I_2. *Allora:*

(a)

$$\mathbf{i}^4 = \mathbf{j}^4 = \mathbf{k}^4 = 1, \quad \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1,$$
$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik},$$
$$\mathbf{i}^3 = -\mathbf{i}, \quad \mathbf{j}^3 = -\mathbf{j}, \quad \mathbf{k}^3 = -\mathbf{k};$$

(b) Q_8 *è un sottogruppo non abeliano di* $GL_2(\mathbb{C})$*;*
(c) i sottogruppi di Q_8 *sono* $\langle\mathbf{i}\rangle$, $\langle\mathbf{j}\rangle$, $\langle\mathbf{k}\rangle$, $Z(Q_8)$ *e sono tutti normali;*
(d) Q_8 *è l'unione insiemistica di tre suoi sottogruppi, cioè* $Q_8 = \langle\mathbf{i}\rangle \cup \langle\mathbf{j}\rangle \cup \langle\mathbf{k}\rangle$.

DIMOSTRAZIONE. (a) È un facile esercizio.

(b) Bisogna verificare che prodotti di elementi di Q_8 sono ancora elementi di Q_8, ricordando che la verifica per l'inverso di un elemento di Q_8 non è necessaria poiché Q_8 è finito, grazie all'esercizio 5.15.

(c) Q_8 è un gruppo di ordine 8, quindi, per il teorema di Lagrange 5.52, i suoi sottogruppi propri possono avere solo ordine 4 o 2. Se un sottogruppo H contiene **i**, allora contiene $\langle\mathbf{i}\rangle$ e quindi o $H = Q_8$ oppure $H = \langle\mathbf{i}\rangle$, poiché $\langle\mathbf{i}\rangle = \{1, i, -i, -1\}$. Analogamente per **i, j, k, -i, -j, -k**. Allora l'unica altra possibilità è che H non contenga nessuno di quegli elementi, cioè $H = \langle -1\rangle$. Infine i primi tre sottogruppi sono normali perché hanno indice 2, grazie all'esercizio 5.40 e il quarto è normale perché è il centro del gruppo Q_8.

(d) Ogni elemento di Q_8 è contenuto in uno dei tre sottogruppi $\langle\mathbf{i}\rangle$, $\langle\mathbf{j}\rangle$, $\langle\mathbf{k}\rangle$. □

Passiamo ora a considerare un esempio di un gruppo lineare infinito. Il sottogruppo definito nel seguente lemma 5.82 si dice *gruppo di Heisenberg* e viene utilizzato in fisica.

Lemma 5.82. *Sia G l'insieme delle matrici* $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ *con $a, b, c \in \mathbb{Z}$. Allora G è un sottogruppo di $GL_3(\mathbb{Q})$ e il centro di G è*

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}.$$

DIMOSTRAZIONE. La matrice identica $I_3 \in G$ ed è facile verificare che

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + a' & b + ac' + b' \\ 0 & 1 & c + c' \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b + ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = I_3.$$

Da questo segue che G è un gruppo e che il centro di G è esattamente

$$\left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}.$$

□

Concludiamo il paragrafo con alcune osservazioni riguardanti i gruppi lineari definiti su campi finiti. Consideriamo l'insieme $\mathbb{Z}_p$ delle classi resto modulo p, ove p è un primo. Allora $(\mathbb{Z}_p, +, \cdot)$ è un campo, che denoteremo con $\mathbb{F}_p$ per ricordare che stiamo parlando della struttura di campo definita sull'insieme $\mathbb{Z}_p$ (F spesso denota un campo, dall'iniziale della parola inglese "field"). Possiamo quindi parlare di spazi vettoriali sul campo $\mathbb{F}_p$. Dalla geometria è noto che ogni spazio vettoriale di dimensione n su $\mathbb{F}_p$ è isomorfo a $\mathbb{F}_p^n$. Inoltre possiamo fissare la base canonica di $\mathbb{F}_p^n$, definita da $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$. Osserviamo infine che uno spazio vettoriale di dimensione n su $\mathbb{F}_p$ ha ordine p^n.

Il gruppo $GL_n(\mathbb{F}_p)$ è finito, in quanto si tratta di un insieme di matrici i cui elementi stanno in un insieme finito. Calcoliamo la cardinalità di $M_n(\mathbb{F}_p)$ e di $GL_n(\mathbb{F}_p)$.

Lemma 5.83. *Sia $\mathbb{F}_p$ il campo con p elementi. Allora:*

(a) $|M_n(\mathbb{F}_p)| = p^{n^2}$;
(b) $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \ldots (p^n - p^{n-2})(p^n - p^{n-1}) = p^{n(n-1)/2}(p^n - 1)(p^{n-1} - 1)(p^{n-2} - 1) \ldots (p^2 - 1)(p - 1)$.

DIMOSTRAZIONE. (a) Per ogni elemento di una matrice di $M_n(\mathbb{F}_p)$ si hanno p scelte e quindi in totale si avranno p^{n^2} possibili matrici.

(b) Ogni matrice $A = (a_{ij}) \in GL_n(\mathbb{F}_p)$ è caratterizzata dalla proprietà $\det(A) \neq 0$. Dalla definizione di determinante questo implica che, se denotiamo con $\alpha_i = (a_{i1} \dots a_{in})$ l'i-esimo vettore riga per $i = 1, \dots, n$, allora i vettori $\alpha_1, \dots, \alpha_n$ sono linearmente indipendenti. Pertanto contiamo quante scelte si hanno per ogni riga. Per la prima riga α_1 abbiamo $p^n - 1$ scelte. Il vettore α_2 non deve appartenere al sottospazio generato da α_1, e quindi abbiamo $p^n - p$ scelte. Il vettore α_i non deve essere combinazione lineare dei precedenti vettori $\alpha_1, \dots, \alpha_{i-1}$ già fissati, cioè non deve appartenere al sottospazio vettoriale da essi generato che deve avere dimensione $i-1$. Quindi si hanno $p^n - p^{i-1}$ scelte per l'i-esimo vettore riga α_i. Concludiamo che

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-2})(p^n - p^{n-1}).$$

□

5.7 Esercizi su gruppi e sottogruppi

Esercizio 5.1 Sia A un gruppo abeliano, a e b elementi di A di ordine rispettivamente m ed n, con $m, n \in \mathbb{Z}$. Allora l'ordine di ab divide mn.

Esercizio 5.2 Sia G un gruppo e siano $a_1, a_2, a_3 \in G$. Provare che l'inverso del prodotto $a_1 a_2 a_3$ è l'elemento $a_3^{-1} a_2^{-1} a_1^{-1}$.

Esercizio 5.3 Sia X un insieme e sia $\triangle$ la differenza simmetrica, cioè l'operazione su $\mathcal{P}(X)$ così definita:

$$A, B \in \mathcal{P}(X), \quad A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Si provi che $(\mathcal{P}(X), \triangle)$ è un gruppo abeliano. Si calcolino i periodi degli elementi di $(\mathcal{P}(X), \triangle)$.

Esercizio 5.4 Se σ è un ciclo, è vero che anche il suo quadrato σ^2 è un ciclo?

Esercizio 5.5 Dimostrare che ogni permutazione in S_3 è un ciclo e le uniche permutazioni in S_4 che non sono cicli sono $(12)(34)$, $(13)(24)$ e $(14)(23)$.

Esercizio 5.6 Scrivere tutte le permutazioni di S_5 e S_6 che non sono cicli.

Esercizio 5.7 Sia σ la permutazione di S_{12} definita come segue:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 6 & 7 & 10 & 12 & 9 & 4 & 3 & 11 & 8 & 2 & 1 \end{pmatrix}.$$

Si trovi la decomposizione in cicli disgiunti delle permutazioni σ, σ^2, σ^3 e σ^5.

Esercizio 5.8 Siano σ e τ le permutazioni di S_{10} definite come segue:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 5 & 7 & 9 & 8 & 10 & 6 & 3 & 1 \end{pmatrix}, \qquad \tau = (23).$$

Si trovi la decomposizione in cicli disgiunti di σ, τ, $\sigma \circ \tau$ e $\tau \circ \sigma$.

Esercizio 5.9 Siano σ e τ le permutazioni di S_8 definite rispettivamente come segue:

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 2\,3\,4\,1\,6\,7\,8\,5 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 5\,8\,7\,6\,3\,2\,1\,4 \end{pmatrix}.$$

Si dimostri che $\sigma\tau = \tau^{-1}\sigma$ e si trovi la decomposizione in cicli disgiunti di σ, τ e $\sigma\tau$.

Esercizio 5.10 Siano $2 \leq n \in \mathbb{N}$ e $\sigma \in S_n$ una permutazione non identica. Se $\sigma = \rho_1 \dots \rho_t$ è la fattorizzazione di σ in cicli disgiunti ρ_i di lunghezze l_i, $i = 1, \dots, t$ rispettivamente, si dimostri che $o(\sigma) = m.c.m.\{l_i : i = 1, \dots, t\}$.

Esercizio 5.11 Sia $X = \{x, y\}$. Si dimostri che il sottogruppo generato da X coincide con l'insieme

$$H = \{x^{n_1}y^{m_1}x^{n_2}y^{m_2} \dots x^{n_k}y^{m_k} : k \in \mathbb{N}_+, n_i, m_i \in \mathbb{Z} \text{ per } i = 1, 2, \dots, k\}.$$

Se x ed y sono permutabili, si dimostri che $\langle X \rangle$ coincide con l'insieme

$$\{x^n y^m : n, m \in \mathbb{Z}\}.$$

Esercizio 5.12 Sia $X = H \cup K$, dove H e K sono sottogruppi di G. Provare che:

(a) il sottogruppo generato da X coincide con l'insieme

$$\{h_1k_1h_2k_2 \dots h_sk_s : s \in \mathbb{N}_+, h_i \in H, k_i \in K \text{ per } i = 1, 2, \dots, s\};$$

(b) se G è abeliano, il sottogruppo generato da X coincide con l'insieme

$$HK = \{hk : h \in H,\ k \in K\}.$$

Esercizio 5.13 Ricavare la conclusione dell'esercizio 5.11 dal lemma 5.31 e dall'esercizio 5.12.

Esercizio 5.14 Si dimostri che l'insieme $\{(12)(34), (13)(24), (14)(23), id\}$ è un sottogruppo di S_4.

Esercizio 5.15 Sia G un gruppo finito. Un sottoinsieme non vuoto H di G è un sottogruppo se H è stabile, cioè se $ab \in H$ per ogni a, b in H.

Esercizio 5.16 Sia G il gruppo delle funzioni reali a variabile reale con la somma, come definito nell'esercizio 4.15. Si dimostri che i seguenti insiemi sono dei sottogruppi di G:

(a) $\mathcal{C}(\mathbb{R}) = \{$funzioni continue $f : \mathbb{R} \to \mathbb{R}\}$;
(b) $\mathcal{D}(\mathbb{R}) = \{$funzioni derivabili $f : \mathbb{R} \to \mathbb{R}\}$;
(c) $\mathcal{I}(\mathbb{R}) = \{$funzioni integrabili $f : \mathbb{R} \to \mathbb{R}\}$.

Esercizio 5.17 Siano G ed H due gruppi e sia $G \times H$ il gruppo prodotto diretto definito nel teorema 4.19. Si dimostri che i seguenti sottoinsiemi sono sottogruppi:

(a) $G_1 = \{(g, 1_H) : g \in G\}$;
(b) $H_1 = \{(1_G, h) : h \in H\}$.

Esercizio 5.18 Sia G un gruppo e sia $G \times G$ il gruppo prodotto diretto definito nel teorema 4.19. Si dimostri che $D = \{(g, g) : g \in G\}$ è un sottogruppo di $G \times G$.

Esercizio 5.19 Sia V uno spazio vettoriale di dimensione 3 sul campo $\mathbb{R}$ generato dai vettori e_1, e_2 ed e_3. Si dimostri che il sottoinsieme $W = \{ae_1 + be_2 : a, b \in \mathbb{R}\}$ è un sottogruppo di V. Si descrivano le classi laterali destre e sinistre di W.

Esercizio 5.20 Sia V uno spazio vettoriale di dimensione n sul campo $\mathbb{R}$ e sia W un sottospazio proprio di V. Si descrivano le classi laterali destre e sinistre di W.

Esercizio 5.21 Sia $n \in \mathbb{N}_+$. Dato il sottogruppo $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ di $(\mathbb{Z}, +)$ si calcoli $[\mathbb{Z} : n\mathbb{Z}]$.

Esercizio 5.22 Per i gruppi $G = (\mathbb{Z}_2, +)$, $(\mathbb{Z}_3, +)$, $(\mathbb{Z}_4, +)$, $(\mathbb{Z}_5, +)$, $(\mathbb{Z}_6, +)$, $(\mathbb{Z}_7, +)$, $(\mathbb{Z}_8, +)$, $(\mathbb{Z}_9, +)$ $(\mathbb{Z}_{10}, +)$ descrivere tutti i sottogruppi H di G e calcolare l'indice $[G : H]$. Determinare qual è il gruppo con il maggior numero di sottogruppi.

Esercizio 5.23 * Sia G un gruppo infinito e H un sottogruppo di G. Provare che

$$|G| = \max\{[G : H], |H|\}.$$

Esercizio 5.24 Si dimostri che $H = \{x + iy \in \mathbb{C} : 5x + 3y = 0\}$ è un sottogruppo del gruppo additivo dei numeri complessi.

Esercizio 5.25 Elencare tutti i sottogruppi di A_4 di ordine 2, 3, 4.

Esercizio 5.26 Elencare tutti i sottogruppi di S_3.

Esercizio 5.27 Si provi che l'insieme

$$S = \{\rho(\cos(2k\pi/3) + i\sin(2k\pi/3)) |\ \rho \in \mathbb{R}, \rho > 0, k \in \mathbb{Z}\}$$

è un sottogruppo di $(\mathbb{C}^*, \cdot, 1)$.

Esercizio 5.28 Sia $\mathbb{Q}$ il campo dei numeri razionali e si consideri il gruppo

$$G = \{(a, b) | a, b \in \mathbb{Q}, a \neq 0\}$$

con l'operazione di moltiplicazione definita dalla posizione

$$(a, b) \cdot (c, d) = (ac, ad + b).$$

(a) Si determini l'unità di G e l'inverso dell'elemento $(a, b) \in G$.
(b) Si verifichi che $H = \{(a, 0) | a \in \mathbb{Q}, a \neq 0\}$ è un sottogruppo di G.

Esercizio 5.29 Dimostrare che se H, K ed L sono sottogruppi di un gruppo abeliano G, non è detto che valga la legge distributiva del prodotto rispetto all'intersezione, come definita prima dell'osservazione 5.41.

Esercizio 5.30 Si deduca dal lemma 5.30 che l'insieme $\mathcal{L}(G)$ dei sottogruppi di G ordinato per inclusione è un reticolo limitato avente G come elemento massimo e $\{1\}$ come minimo.

Esercizio 5.31 Sia H un sottogruppo di G e g un elemento di G. Si dimostri che H^g è un sottogruppo di G.

Esercizio 5.32 Sia $Z(G)$ il centro di un gruppo G. Si dimostri che:

(a) $Z(G) = G$ se e solo se G è abeliano;
(b) se G è un gruppo semplice non abeliano, allora $Z(G) = \{1\}$.

Esercizio 5.33 Sia $Z(G)$ il centro di un gruppo G. Se H è un sottogruppo di G, si dimostri che $Z(H)$ contiene $Z(G) \cap H$. Si mostri con un esempio che l'inclusione può essere stretta.

Esercizio 5.34 Siano $A, B \in \mathrm{M}_n(K)$, $n \in \mathbb{N}_+$; provare che $(AB)^t = B^t A^t$.

Esercizio 5.35 Si dimostri che l'insieme $G = GL_3(\mathbb{Z})$ delle matrici quadrate di ordine 3 a coefficienti interi con determinante ± 1 forma un sottogruppo di $GL_3(\mathbb{R})$.

Esercizio 5.36 Sia G il gruppo $GL_3(\mathbb{F}_2)$.

(a) Si calcoli l'ordine di G;
(b) si descriva il centro di G;
(c) sia N l'insieme delle matrici $\begin{pmatrix} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}$ con $a, b, c \in \mathbb{F}_2$. Si dimostri che N è un sottogruppo di G.

Esercizio 5.37 Sia G il gruppo $GL_2(\mathbb{F}_3)$.

(a) Si calcoli l'ordine di G;
(b) si descriva il centro di G;
(c) si trovino almeno due sottogruppi di ordine 3 di G.

Esercizio 5.38 Sia G un gruppo e Z il suo centro. Dimostrare che:

(a) per ogni elemento a di G il sottogruppo di G generato da Z e a è abeliano;
(b) se $ab \in Z(G)$, allora $ab = ba$;
(c) l'implicazione inversa in (b) non vale in generale.

Esercizio 5.39 Determinare $Z(S_2)$, $Z(S_3)$, $Z(S_4)$.

Esercizio 5.40 Sia G un gruppo e sia N un sottogruppo di G di indice 2.

(a) Dimostrare che N è normale.
(b) Dare un esempio di un gruppo G e di un sottogruppo N di G di indice 3 che non sia normale.

Esercizio 5.41 Siano H ed N sottogruppi di un gruppo finito G, con $H \leq N \leq G$. Allora $[G : H] = [G : N][N : H]$.

Esercizio 5.42 Siano G un gruppo finito, H un suo sottogruppo di indice p, con p primo. Supponiamo che esista $g \in G \setminus H$ tale che $gH = Hg$. Dimostrare che H è normale in G.

Esercizio 5.43 Sia Q_8 il gruppo dei quaternioni definito nel lemma 5.81.

(a) Si provi (a) del lemma 5.81.
(b) Si consideri il sottogruppo $V = \langle (12)(34), (13)(24) \rangle$ di S_4. Si provi che V è l'unione di tre sottogruppi propri e si calcoli $|V|$.

Esercizio 5.44 Siano K campo e $H = \{A \in GL_n(K) : A^t = A\}$ l'insieme delle matrici simmetriche di $GL_n(K)$, si veda la definizione 5.78. Si dimostri che H non è un sottogruppo di $GL_n(K)$, se $n > 1$.

Esercizio 5.45 Sia K un campo. Determinare l'intersezione $\mathrm{O}_n(K) \cap \mathrm{T}_n^-(K)$, dove $\mathrm{T}_n^-(K)$ è il sottogruppo delle matrici triangolari inferiori.

Esercizio 5.46 Sia K un campo. Dimostrare che $\mathrm{O}_2(K)$ non è un sottogruppo normale di $\mathrm{GL}_2(K)$.

Esercizio 5.47 Si considerino i seguenti insiemi di matrici in $SL_2(\mathbb{R})$:

$$U^+ = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}, \quad U^- = \left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} : x \in \mathbb{R} \right\},$$

$$D = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} : x \in \mathbb{R}, x \neq 0 \right\}.$$

(a) Dimostrare che U^+, U^- e D sono sottogruppi di $SL_2(\mathbb{R})$. Determinare quali di questi sottogruppi sono normali.
(b) Descrivere l'insieme U^-DU^+ dei prodotti

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$$

al variare di $x, y, d \in \mathbb{R}$ con $d \neq 0$.
(c) Sia

$$\varepsilon = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Dimostrare che

$$SL_2(\mathbb{R}) = U^-DU^+ \cup U^-D\varepsilon.$$

Esercizio 5.48 Sia G il gruppo di Heisenberg definito nel lemma 5.82 e sia N l'insieme delle matrici

$$\begin{pmatrix} 1 & 2b & 2c \\ 0 & 1 & 2a \\ 0 & 0 & 1 \end{pmatrix}$$

con $a, b, c \in \mathbb{Z}$. Si dimostri che N è un sottogruppo normale di G.

Esercizio 5.49 Si calcoli l'ordine del centro del gruppo $G = GL_2(\mathbb{F}_p)$, dove p è un numero primo.

Esercizio 5.50 Sia G un gruppo e H, K sottogruppi di G. Si dimostri che ogni elemento di G si scrive in modo unico come prodotto di un elemento di H e di un elemento di K se e solo se $G = HK$ e $H \cap K = \{1\}$.

Esercizio 5.51 * Si consideri un quadrato inscritto in un cerchio di raggio 1 e centro l'origine del piano complesso. Siano σ la rotazione antioraria di $\pi/2$ radianti con centro l'origine del piano complesso e τ la riflessione rispetto ad una delle diagonali del quadrato. Allora $\sigma, \tau \in S_{\mathbb{C}}$ e σ, τ trasformano il quadrato in se stesso.

(a) Quali sono tutte e sole le altre rotazioni del cerchio su se stesso che trasformano il quadrato in sé?
(b) Qual è l'ordine del gruppo ciclico $\langle\sigma\rangle$?
(c) Sia τ il ribaltamento del quadrato rispetto ad una delle sue diagonali. Qual è l'ordine di τ?
(d) Si provi che $\tau \circ \sigma \circ \tau = \sigma^{-1}$.
(e) Che ordine ha il gruppo $G = \langle\sigma, \tau\rangle$?
(f) Qual è il centro di G?

Il gruppo G definito in (e) viene chiamato *gruppo diedrale* e denotato con D_8.

Esercizio 5.52 * Si consideri un pentagono regolare inscritto in un cerchio di raggio 1 e centro l'origine del piano complesso. Siano σ la rotazione antioraria di $2\pi/5$ radianti con centro l'origine del piano complesso e τ il ribaltamento del pentagono rispetto ad uno dei suoi assi di simmetria. Allora $\sigma, \tau \in S_{\mathbb{C}}$ e σ, τ trasformano il pentagono in se stesso.

(a) Quali sono tutte e sole le altre rotazioni del cerchio su se stesso che trasformano il pentagono in sé?
(b) Qual è l'ordine del gruppo ciclico $\langle\sigma\rangle$?
(c) Qual è l'ordine di τ?
(d) Si provi che $\tau \circ \sigma \circ \tau = \sigma^{-1}$.
(e) Provare che il gruppo $G = \langle\sigma, \tau\rangle$ ha ordine 10 e che $Z(G) = \{1\}$.

Esercizio 5.53 * Si consideri un esagono regolare inscritto in un cerchio di raggio 1 e centro l'origine del piano complesso. Siano σ la rotazione antioraria di $\pi/3$ radianti con centro l'origine del piano complesso e τ il ribaltamento dell'esagono rispetto ad una delle sue diagonali grandi. Allora $\sigma, \tau \in S_{\mathbb{C}}$ e σ, τ trasformano l'esagono in se stesso.

(a) Quali sono tutte e sole le altre rotazioni del cerchio su se stesso che trasformano l'esagono in sé?
(b) Qual è l'ordine del gruppo ciclico $\langle\sigma\rangle$?
(c) Qual è l'ordine di τ?
(d) Si provi che $\tau \circ \sigma \circ \tau = \sigma^{-1}$.
(e) Provare che il gruppo $G = \langle\sigma, \tau\rangle$ ha ordine 12 e che $|Z(G)| = 2$.

Esercizio 5.54 * Si consideri un poligono regolare P di sette lati inscritto in un cerchio di raggio 1 e centro l'origine del piano complesso. Siano σ la rotazione antioraria di $2\pi/7$ radianti con centro l'origine del piano complesso e τ il ribaltamento di P rispetto ad uno dei suoi assi di simmetria. Allora $\sigma, \tau \in S_{\mathbb{C}}$ e σ, τ trasformano P in se stesso.

(a) Quali sono tutte e sole le altre rotazioni del cerchio su se stesso che trasformano P in sé?
(b) Qual è l'ordine del gruppo ciclico $\langle\sigma\rangle$?
(c) Qual è l'ordine di τ?
(d) Si provi che $\tau \circ \sigma \circ \tau = \sigma^{-1}$.
(e) Provare che il gruppo $G = \langle\sigma, \tau\rangle$ ha ordine 14 e che $Z(G) = \{1\}$.

Esercizio 5.55 Sia G un gruppo. Definiamo una relazione $\sim$ in G ponendo

$$x \sim y \quad \text{se e solo se } \langle x\rangle = \langle y\rangle.$$

(a) Si verifichi che $\sim$ è una relazione di equivalenza.
(b) Si verifichi che per ogni $g \in G$ risulta $g \sim g^{-1}$.
(c) È vero che se $g \in G$ è aperiodico allora la classe $[g]_\sim$ di g rispetto a $\sim$ contiene esattamente due elementi?
(d) * Si dimostri che se G è infinito, allora G ha infiniti sottogruppi.

Esercizio 5.56 Sia G un gruppo e $x, y \in G$. Provare che $o(xy) = o(yx)$.

Esercizio 5.57 Dato un gruppo G possiamo definire la relazione $x \sim_G y$ se e solo se esiste $g \in G$ tale che $y = x^g$. Dimostrare che $\sim$ è di equivalenza.

Esercizio 5.58 Sia $G = GL_3(\mathbb{R})$, si consideri il sottoinsieme

$$H = \left\{ \begin{pmatrix} 1 & n & \frac{n^2-n}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}, \ n \in \mathbb{Z} \right\}.$$

(a) Si dimostri che H è un sottogruppo di G.
(b) Si provi che H è ciclico e se ne trovi un generatore.

Omomorfismi e prodotti diretti di gruppi

Cominciamo il capitolo con la costruzione del gruppo quoziente G/N di un gruppo G rispetto ad un sottogrupo normale N. Il secondo paragrafo è dedicato agli omomorfismi di gruppo, nucleo e immagine di un omomorfismo. Esempio rilevante è l'omomorfismo canonico $\pi : G \to G/N$ che mette in relazione un gruppo G con il suo gruppo quoziente G/N. Nel terzo paragrafo dimostriamo il primo teorema di omomorfismo secondo il quale tutti gli omomorfismi suriettivi hanno la forma $\pi : G \to G/N$, a meno di un opportuno isomorfismo. Seguono gli altri due teoremi di omomorfismo che chiarischicono la struttura dei quozienti dei sottogruppi e dei quozienti del gruppo G. Il gruppo degli automorfismi $\text{Aut}(G)$ di un gruppo G viene studiato nel quarto paragrafo, in cui viene dimostrato anche il teorema di Cayley, che afferma che ogni gruppo è isomorfo ad un sottogruppo di un gruppo di permutazioni. Infine il quinto paragrafo è dedicato ai prodotti diretti dei gruppi.

6.1 Quozienti di gruppi

Sia G un gruppo e sia N un sottogruppo normale di G. Nel paragrafo 5.4 sono state definite due relazioni di equivalenza relative al sottogruppo N, la relazione $\sim$ nel lemma 5.44 e la relazione $\sim'$ nel successivo lemma 5.45. Dal fatto che N è normale segue che queste due relazioni di equivalenza coincidono. Questo permette di definire nell'insieme quoziente G/N delle classi laterali un'operazione binaria che lo rende un gruppo.

Teorema 6.1. *Siano G un gruppo e N un sottogruppo normale di G. Nell'insieme delle classi laterali di G/N si definisca il prodotto $xN \cdot yN = xyN$. Allora $(G/N, \cdot)$ è un gruppo, detto gruppo quoziente di G su N.*

DIMOSTRAZIONE. L'operazione $\cdot$ è ben definita, cioè se $xN = x_1N$ e $yN = y_1N$, allora $xyN = x_1y_1N$. Infatti si ha $x_1 = xh$ e $y_1 = yh'$ per opportuni $h, h' \in N$. Allora per il lemma 5.64 e l'osservazione 5.65 si ha $x_1y_1 = xhyh' = xyh''h' \in xyN$, dove h'' è un opportuno elemento di N. Dunque $xyN = x_1y_1N$.

Verifichiamo la legge associativa. Siano $x, y, z \in G$, allora

$$(xN \cdot yN) \cdot zN = (xyN) \cdot zN = ((xy)z)N =$$

$$= (x(yz))N = xN \cdot (yzN) = xN \cdot (yN \cdot zN).$$

La classe N dell'elemento 1 è l'elemento neutro di $(G/N, \cdot)$, infatti per ogni $x \in G$ si ha:

$$N \cdot xN = 1N \cdot xN = (1 \cdot x)N = xN \text{ e } xN \cdot N = xN \cdot 1N = (x \cdot 1)N = Nx.$$

Infine se $x \in G$,

$$(xN) \cdot (x^{-1}N) = (x \cdot x^{-1})N = 1N = N \quad \text{e}$$

$$(x^{-1}N) \cdot (xN) = (x^{-1}xN) = 1N = N,$$

quindi la classe $x^{-1}N$ è l'inversa della classe xN. □

Esempio 6.2. Sia $m > 1$ un intero. Allora $m\mathbb{Z} = \langle m \rangle$ è un sottogruppo normale di $\mathbb{Z}$. La relazione di equivalenza associata al sottogruppo $m\mathbb{Z}$ è definita da $x \sim y$ se e solo se $y - x \in m\mathbb{Z}$, ovvero $x \equiv_m y$. In altre parole, in questo caso troviamo la congruenza modulo m introdotta nel paragrafo 3.5. Quindi le classi laterali $x + m\mathbb{Z}$ coincidono con le classi $[x]_m$ dei resti modulo m. Perciò il gruppo quoziente $(\mathbb{Z}/m\mathbb{Z}, +)$ in questo caso coincide con il gruppo $(\mathbb{Z}_m, +)$ introdotto in precedenza.

Osserviamo che gli elementi di un insieme quoziente sono classi di equivalenza che possono avere diversi rappresentanti. Pertanto, quando si definisce l'immagine di una classe dando l'immagine di un rappresentante della classe, bisogna verificare che poi la funzione sia *ben definita*, cioè che se si sceglie un altro rappresentante l'immagine sia effettivamente la stessa.

Vediamolo meglio con un esempio.

Esempio 6.3. Sia $(\mathbb{Z}_6, +)$ il gruppo delle classi resto modulo 6 e $(\mathbb{Z}_8, +)$ il gruppo delle classi resto modulo 8. Sia $f : \mathbb{Z}_6 \to \mathbb{Z}_8$ definita da $f([x]_6) = [2x]_8$. Osserviamo che $[1]_6 = [7]_6$, mentre $f([1]_6) = [2]_8 \neq f([7]_6) = [6]_8$; quindi f non è ben definita.

Sia $g : \mathbb{Z}_6 \to \mathbb{Z}_8$ definita da $g([x]_6) = [4x]_8$. Se $[x]_6 = [y]_6$, allora $x = y + 6k$ per qualche $k \in \mathbb{Z}$. Quindi $4x = 4y + 24k$ e pertanto $[4x]_8 = [4y]_8$. Dunque g è ben definita.

Calcoliamo ora la cardinalità del gruppo quoziente di un gruppo finito.

Osservazione 6.4. L'ordine di ogni quoziente di un gruppo finito G divide l'ordine del gruppo. Infatti se il quoziente ha la forma G/N per qualche sottogruppo normale N di G, allora $|G/N| = [G : N]$. Pertanto $[G : N]$ divide $|G|$ per il corollario 5.53.

6.2 Omomorfismi di gruppo

Un omomorfismo tra due gruppi G ed H è un'applicazione da G in H che *rispetta* la struttura di gruppo. Più precisamente:

Definizione 6.5. Se G ed H sono gruppi, un *omomorfismo di gruppi* o *morfismo* di G in H è un'applicazione $\varphi\colon G \to H$ tale che per ogni $a, b \in G$ risulti $\varphi(ab) = \varphi(a)\varphi(b)$.
Se φ è anche biettiva, φ si dice un *isomorfismo*.

Nei gruppi moltiplicativi si usa talvolta la notazione g^φ e H^φ per indicare $\varphi(g)$ e $\varphi(H)$, dove $g \in G$ e H è un sottoinsieme di G.
Proviamo alcune proprietà degli omomorfismi.

Lemma 6.6. *Sia $\varphi : G \to H$ un omomorfismo tra due gruppi G e H. Allora:*

(a) $\varphi(1_G) = 1_H$*;*
(b) $\varphi(x^{-1}) = (\varphi(x))^{-1}$ *per ogni* $x \in G$*;*
(c) $\varphi(x^n) = (\varphi(x))^n$ *per ogni* $x \in G$, $n \in \mathbb{Z}$.

DIMOSTRAZIONE. (a) Poiché $\varphi(1_G)1_H = \varphi(1_G) = \varphi(1_G1_G) = \varphi(1_G)\varphi(1_G)$, applicando la legge di cancellazione si ottiene $1_H = \varphi(1_G)$.
(b) Dal fatto che $1_H = \varphi(1_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, per l'unicità dell'inverso, segue che $(\varphi(x))^{-1} = \varphi(x^{-1})$.
(c) Lo proviamo per induzione su n, nel caso in cui $n \geq 0$. Il caso $n = 0$ lo abbiamo provato in (a). Supponiamo ora vero l'enunciato per $n - 1$; allora

$$\varphi(x^n) = \varphi(x^{n-1}x) = \varphi(x^{n-1})\varphi(x) = (\varphi(x))^{n-1}\varphi(x) = (\varphi(x))^n.$$

Per $n < 0$ si pone $x^n = (x^{-1})^{-n}$ e si utilizzano (b) e la formula dimostrata per $n > 0$. □

Diamo una relazione tra i generatori di un gruppo e i generatori dell'immagine tramite un omomorfismo.

Lemma 6.7. *Siano G, H gruppi, $X \subseteq G$ e $f : G \to H$ un omomorfismo suriettivo;*

(a) se X genera G, allora $f(X)$ genera H;
(b) se G è ciclico, allora H è ciclico.

DIMOSTRAZIONE. (a) Sia $G = \langle X \rangle$. Se $h \in H$, esiste $g \in G$ tale che $h = f(g)$. Essendo $G = \langle X \rangle$ esistono $x_1, \dots, x_r \in X \cup X^{-1}$ tali che $g = x_1 \dots x_r$. Allora

$$y = f(g) = f(x_1 \dots x_r) = f(x_1) \dots f(x_r) \in \langle f(X) \rangle$$

che prova $H = \langle f(X) \rangle$.
(b) Se G è ciclico, esiste $g \in G$ tale che $G = \langle g \rangle$ e quindi $H = \langle f(g) \rangle$ è ciclico.
□

Dato un omomorfismo $\varphi : G \to H$, possiamo definire l'*immagine* di φ

$$\operatorname{Im}(\varphi) = \varphi(G) = G^{\varphi} = \{x^{\varphi} : x \in G\}$$

e il *nucleo* di φ

$$\ker(\varphi) = \{x \in G : x^{\varphi} = 1_H\}.$$

Proposizione 6.8. *Sia* $\varphi\colon G \to H$ *un omomorfismo di gruppi. Allora:*

(a) $\operatorname{Im}(\varphi)$ *è un sottogruppo di* H*;*
(b) $\ker(\varphi)$ *è un sottogruppo normale di* G*.*

DIMOSTRAZIONE. (a) $\operatorname{Im}(\varphi)$ non è vuoto perché $\varphi(1_G) = 1_H$. Dati $y, z \in \operatorname{Im}(\varphi)$, si ha $y = \varphi(x)$ e $z = \varphi(t)$ per qualche $x, t \in G$. Allora

$$y^{-1}z = (\varphi(x))^{-1}\varphi(t) = \varphi(x^{-1})\varphi(t) = \varphi(x^{-1}t) \in \operatorname{Im}(\varphi).$$

Quindi per il lemma 5.29 $\operatorname{Im}(\varphi)$ è un sottogruppo.

(b) Per (a) del lemma 6.6 si ha $1_G \in \ker\varphi$. Inoltre, se $x, y \in \ker\varphi$, si ha

$$\varphi(x^{-1}y) = \varphi(x^{-1})\varphi(y) = \varphi(x)^{-1}1_H = 1_H,$$

poiché $\varphi(x) = \varphi(y) = 1$. Per il lemma 5.29 $\ker\varphi$ è un sottogruppo di G. Verifichiamo che $\ker\varphi$ è un sottogruppo normale. Sia $x \in G$ e $a \in \ker\varphi$. Allora

$$\varphi(xax^{-1}) = \varphi(x)\varphi(a)\varphi(x^{-1}) = \varphi(x)1\varphi(x)^{-1} = \varphi(xx^{-1}) = 1,$$

quindi $xax^{-1} \in \ker\varphi$. □

Lemma 6.9. *Sia* $\varphi : G \to G_1$ *un omomorfismo di gruppi. Allora:*

(a) $\varphi(x) = \varphi(y)$ *per* $x, y \in G$ *se e solo se* $y \in x\ker\varphi$*;*
(b) $\varphi^{-1}(\varphi(x)) = x\ker\varphi$ *per ogni* $x \in G$*;*
(c) φ *è iniettivo se e solo se* $\ker(\varphi) = \{1\}$.

DIMOSTRAZIONE. (a) Abbiamo

$$\varphi(x) = \varphi(y) \iff \varphi(x)^{-1}\varphi(y) = 1 \iff \varphi(x^{-1})\varphi(y) = 1 \iff$$
$$\varphi(x^{-1}y) = 1 \iff x^{-1}y \in \ker\varphi \iff y \in x\ker\varphi.$$

(b) Segue da (a).

(c) Da (b) segue che $\ker(\varphi) = \{1\}$ se φ è iniettivo. Se $\ker(\varphi) = \{1\}$, allora (a) implica che φ è iniettivo. □

Osservazione 6.10. L'insieme delle classi laterali $G/\ker\varphi$ risulta essere l'insieme quoziente definito in 1.47 rispetto alla relazione di equivalenza definita nel lemma 5.44.

Vediamo ora che ogni sottogruppo normale risulta essere il nucleo di qualche omomorfismo.

Esempio 6.11. Siano G un gruppo ed N un sottogruppo normale di G. Si consideri l'applicazione canonica $\pi : G \to G/N$ definita da $\pi(x) = xN$. È facile vedere che π è un omomorfismo. Inoltre π è suriettivo e $\ker \pi = N$. Chiameremo $\pi : G \to G/N$ *omomorfismo canonico.*

Abbiamo già visto che il nucleo di un omomorfismo è un sottogruppo normale. L'esempio 6.11 dimostra che in effetti i sottogruppi normali sono in biezione con i nuclei di omomorfismi.

Se $K \leq G$, allora denotiamo con KN/N il sottoinsieme $\pi(K) = \{kN : k \in K\}$ di G/N. Vedremo nel seguito che il sottoinsieme $KN/N = \pi(K)$ è un sottogruppo di G/N.

6.3 I teoremi di omomorfismo per i gruppi

In questa sezione vogliamo presentare i teoremi di omomorfismo che mettono in luce le relazioni esistenti tra i gruppi quozienti e gli omomorfismi.

Teorema 6.12. *Sia $\varphi : G \to H$ un omomorfismo e $\pi : G \to G/\ker\varphi$ l'omomorfismo canonico. Allora:*

(a) esiste un omomorfismo iniettivo $\widetilde{\varphi} : G/\ker\varphi \to H$ tale che $\widetilde{\varphi} \circ \pi = \varphi$;
(b) $\widetilde{\varphi}$ è un isomorfismo se e solo se φ è suriettivo.

DIMOSTRAZIONE. Definiamo l'applicazione $\widetilde{\varphi}$ ponendo per ogni $x \in G$

$$\widetilde{\varphi}(x \ker\varphi) = \varphi(x).$$

Allora per l'osservazione 6.10 e il teorema 1.49 la funzione $\widetilde{\varphi}$ è ben definita e vale $\widetilde{\varphi} \circ \pi = \varphi$.

Per vedere che $\widetilde{\varphi}$ è un omomorfismo notiamo che

$$\widetilde{\varphi}(x \ker\varphi \cdot y \ker\varphi) = \widetilde{\varphi}(xy \ker\varphi) = \varphi(xy) = \varphi(x)\varphi(y) = \widetilde{\varphi}(x \ker\varphi)\widetilde{\varphi}(y \ker\varphi).$$

Inoltre, se $\widetilde{\varphi}(x \ker\varphi) = 1$, allora $\varphi(x) = 1$ e quindi $x \in \ker\varphi$. Pertanto $\widetilde{\varphi}$ è iniettivo. Questo conclude la dimostrazione del punto (a).

Per il punto (b) basta notare che essendo $\widetilde{\varphi}$ iniettivo, $\widetilde{\varphi}$ è un isomorfismo se e solo se $\widetilde{\varphi}$ è suriettivo. Poiché π è suriettivo, questo è equivalente al fatto che $\varphi = \widetilde{\varphi} \circ \pi$ sia suriettivo. □

Ricaviamo immediatamente il seguente corollario.

Corollario 6.13. (Primo teorema di omomorfismo) *Sia $\varphi : G \to H$ un omomorfismo di gruppi. Allora*

$$G/\ker\varphi \cong \operatorname{Im}(\varphi).$$

Poiché questo corollario si usa prevalentemente nel caso di omomorfismi suriettivi, diamo esplicitamente anche questo caso particolare.

Corollario 6.14. *Sia $\varphi : G \to H$ un omomorfismo suriettivo di gruppi. Allora*

$$H \cong G/\ker\varphi.$$

L'unico vincolo per un'applicazione suriettiva $X \to Y$ tra insiemi finiti è dato dal principio di Dirichlet 1.38 ed è $|X| \geq |Y|$. Dal corollario 6.14 ricaviamo informazioni molto più precise su queste cardinalità nel caso di *omomorfismo* di gruppi finiti.

Corollario 6.15. *Sia $\varphi : G \to H$ un omomorfismo suriettivo di gruppi. Se G è finito, allora $|\ker\varphi|$ e $|H|$ dividono $|G|$.*

DIMOSTRAZIONE. Sia $N = \ker\varphi$. Allora $|N|$ divide $|G|$ per il corollario 5.53. Per il corollario 6.14 $H \cong G/\ker\varphi$ e quindi possiamo applicare l'osservazione 6.4. □

Il seguente teorema prende il nome di **teorema di corrispondenza** e mette in relazione i sottogruppi di un gruppo con le loro immagini tramite un omomorfismo.

Teorema 6.16. *Sia $\varphi : G \to H$ un omomorfismo di gruppi e $N = \ker\varphi$.*

(a) Per ogni $K \leq G$ risulta $\varphi(K) \leq H$; in particolare $\varphi(G) \leq H$. Inoltre,

$$\text{se } K \trianglelefteq G, \quad \text{allora } \varphi(K) \trianglelefteq \varphi(G).$$

(b) Per ogni $L \leq H$ risulta $N \leq \varphi^{-1}(L) \leq G$. Inoltre,

$$\text{se } L \trianglelefteq H, \quad \text{allora } \varphi^{-1}(L) \trianglelefteq G.$$

(c) Per ogni $K \leq G$, si ha

$$\varphi^{-1}(\varphi(K)) = KN/N = \{xN : x \in K\}$$

e

$$\varphi(\varphi^{-1}(L)) = L \cap \varphi(G) \text{ per ogni } L \leq H.$$

DIMOSTRAZIONE. (a) Sia $K \leq G$. Allora $1_G \in K$ e pertanto $1_H = \varphi(1_G) \in \varphi(K)$. Se $u, v \in \varphi(K)$, allora esistono $x, y \in K$ tali che $u = \varphi(x)$ e $v = \varphi(y)$. Ora

$$u^{-1}v = \varphi(x)^{-1}\varphi(y) = \varphi(x^{-1})\varphi(y) = \varphi(x^{-1}y) \in \varphi(K),$$

poiché $x^{-1}y \in K$ in quanto $K \leq G$. Supponiamo $K \trianglelefteq G$. Sia $u \in \varphi(G)$ e $v \in \varphi(K)$; allora $u = \varphi(x)$ e $v = \varphi(y)$ con $x \in G$ e $y \in K$. Si ha $xyx^{-1} \in K$ poiché $K \trianglelefteq G$, quindi

$$uvu^{-1} = \varphi(xyx^{-1}) \in \varphi(K).$$

(b) Analogamente al punto (a) si dimostra che $\varphi^{-1}(L) \leq G$ per ogni $L \leq H$. Poiché $N = \varphi^{-1}(1)$, si ha $N \leq \varphi^{-1}(L)$. Supponiamo ora $L \trianglelefteq H$. Sia $x \in G$ e $z \in \varphi^{-1}(L)$. Allora $\varphi(z) \in L$ e quindi

$$\varphi(xzx^{-1}) = \varphi(x)\varphi(z)\varphi(x)^{-1} \in L$$

poiché $L \trianglelefteq H$. Questo implica $xzx^{-1} \in \varphi^{-1}(L)$ e prova che $\varphi^{-1}(L) \trianglelefteq G$.

(c) Osserviamo che $x \in \varphi^{-1}(\varphi(K))$ se e solo se $\varphi(x) \in \varphi(K)$. In altre parole $x \in \varphi^{-1}(\varphi(K))$ se e solo se $\varphi(x) = \varphi(y)$ per qualche $y \in K$. Per il lemma 6.9(a), $x \in yN$ per qualche $y \in K$. Questo dimostra che

$$\varphi^{-1}(\varphi(K)) = \bigcup_{y \in K} yN = KN.$$

Resta da notare che $\varphi(\varphi^{-1}(L)) \subseteq L$ e $\varphi(\varphi^{-1}(L)) \subseteq \varphi(G)$. Da queste due inclusioni segue immediatamente

$$\varphi(\varphi^{-1}(L)) \subseteq L \cap \varphi(G).$$

L'inclusione

$$L \cap \varphi(G) \subseteq \varphi(\varphi^{-1}(L))$$

è ovvia. □

Corollario 6.17. *Siano $\varphi : G \to H$ un omomorfismo di gruppi e $N = \ker\varphi$. Siano inoltre*

(a) S l'insieme dei sottogruppi di G contenenti *N e*
(b) S' l'insieme dei sottogruppi di H contenuti in *$\varphi(G)$.*

Allora l'applicazione che ad ogni $K \in S$ associa $\varphi(K)$ è una biezione tra S e S'. Inoltre $K \in S$ è normale in G se e solo se $\varphi(K) \in S'$ è normale in $\varphi(G)$.

DIMOSTRAZIONE. Poiché $\varphi(K) \in S'$ per ogni $K \in S$, si definisce un'applicazione $\Phi : S \to S'$ ponendo $\Phi(K) = \varphi(K)$. Per (b) e (c) del teorema 6.16, $\varphi^{-1}(L) \in S$ e $L = \varphi(\varphi^{-1}(L))$ per ogni $L \leq \varphi(G)$. Quindi Φ è suriettiva. Per vedere che Φ è anche iniettiva prendiamo $K, K_1 \in S$ con

$$\Phi(K) = \varphi(K) = \varphi(K_1) = \Phi(K_1).$$

Di nuovo per il punto (c) del teorema 6.16 e dal fatto che $N \leq K$, si ha

$$K = \varphi^{-1}(\varphi(K)) = \varphi^{-1}(\varphi(K_1)) = K_1.$$

Osserviamo infine che l'ultimo enunciato viene direttamente dal teorema 6.16 (a) e (b), osservando che $K = \varphi^{-1}(\varphi(K))$. □

Un caso particolare dell'ultimo corollario ha rilevanza particolare. Si tratta dell'omomorfismo canonico $\pi : G \to G/N$ rispetto ad un sottogruppo normale N di un gruppo G.

Corollario 6.18. (Secondo teorema di omomorfismo) *Siano K un sottogruppo ed N un sottogruppo normale di un gruppo G. Allora $N \cap K \trianglelefteq K$ e*

$$K/K \cap N \cong KN/N.$$

DIMOSTRAZIONE. Consideriamo la restrizione $\varphi = \pi|_K : K \to \varphi(K)$ dell'omomorfismo $\pi : G \to G/N$. Poiché $\varphi(K) = \pi(KN)$, il sottogruppo $\varphi(K)$ coincide con il quoziente KN/N. D'altra parte

$$\ker\varphi = \{x \in K : \varphi(x) = 1\} = K \cap \ker\varphi = K \cap N.$$

Per il primo teorema di omomorfismo 6.13 risulta $K/K \cap N \cong KN/N$. □

Corollario 6.19. *Siano $\varphi : G \to H$ un omomorfismo suriettivo di gruppi, $N = \ker\varphi$ e K sottogruppo di G, con $N \le K \le G$. Allora $K \trianglelefteq G$ se e solo se $\varphi(K) \trianglelefteq H$; in tal caso*

$$G/K \cong H/\varphi(K).$$

DIMOSTRAZIONE. Segue dal corollario 6.17. Per dimostrare l'isomorfismo

$$G/K \cong H/\varphi(K)$$

si consideri l'omomorfismo canonico $\pi' : H \to H/\varphi(K)$ e sia

$$\widetilde{\varphi} = \pi' \circ \varphi : G \to H/\varphi(K).$$

Allora

$$\ker\widetilde{\varphi} = \{x \in G : \widetilde{\varphi}(x) = 1_{H/\varphi(K)}\} = \{x \in G : \varphi(x) \in \varphi(K)\} = K.$$

Per il corollario 6.14 $G/\ker\widetilde{\varphi} = G/K \cong H/\varphi(K)$. □

Dimostriamo infine il terzo teorema di omomorfismo, che prende in considerazione due sottogruppi normali di un gruppo G e ne studia i rispettivi quozienti.

Corollario 6.20. (Terzo teorema di omomorfismo) *Siano N, K sottogruppi normali di un gruppo G e $N \le K$. Allora*

$$K/N \trianglelefteq G/N \quad e \quad G/K \cong (G/N)/(K/N).$$

DIMOSTRAZIONE. Ovviamente, $K = KN$ in quanto $N \le K$. Sia $\pi_1 : G \to G/N$ la proiezione canonica relativa ad N. Per il corollario 6.19 il sottogruppo $\pi_1(K) = KN/N = K/N$ è un sottogruppo normale di G/N. Ora l'isomorfismo $G/K \cong (G/N)/(K/N)$ segue immediatamente dal corollario precedente applicato all'omomorfismo $\pi_1 : G \to G/N$. □

Applichiamo i teoremi di corrispondenza per determinare tutti i sottogruppi di $\mathbb{Z}_m$.

Esempio 6.21. Applicando i risultati precedenti al caso $G = \mathbb{Z}$, $N = m\mathbb{Z}$ e π la proiezione canonica da $\mathbb{Z}$ in $\mathbb{Z}_m$ si ricava la seguente descrizione dei sottogruppi di $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Sia $L \le \mathbb{Z}_m$. Per $K = \pi^{-1}(L)$ si ha $K = n\mathbb{Z}$ per qualche $n > 0$. Poiché $m\mathbb{Z} \le n\mathbb{Z}$, si ha $m \in n\mathbb{Z}$ e di conseguenza n divide m. Quindi i sottogruppi L di $\mathbb{Z}_m$ hanno la forma $L = n\mathbb{Z}/m\mathbb{Z}$ per qualche n che divide m. Per esempio i soli sottogruppi propri non banali di $\mathbb{Z}_6$ sono $2\mathbb{Z}/6\mathbb{Z}$ e $3\mathbb{Z}/6\mathbb{Z}$.

6.4 Il gruppo degli automorfismi di un gruppo

L'insieme di tutti gli omomorfismi di G in H si denota con $\mathrm{Hom}(G, H)$. Questo insieme non è mai vuoto, infatti esiste sempre un omomorfismo da un gruppo G ad un gruppo H: l'omomorfismo banale $b : G \to H$ che manda ogni elemento di G nell'identità 1_H di H.

Un omomorfismo di un gruppo G in se stesso si dice un *endomorfismo* di G, se l'omomorfismo è biettivo si dice un *automorfismo*.

Lemma 6.22. *Sia G un gruppo. L'insieme*

$$\mathrm{End}(G) = \{\varphi : G \to G : \varphi \text{ è un omomorfismo}\}$$

con la composizione di applicazioni è un monoide.

DIMOSTRAZIONE. Siano $\varphi, \psi \in \mathrm{End}(G)$; allora per ogni $x, y \in G$ si ha

$$(\varphi \circ \psi)(xy) = \varphi(\psi(xy)) = \varphi(\psi(x)\psi(y)) =$$
$$= \varphi(\psi(x))\varphi(\psi(y)) = (\varphi \circ \psi)(x)(\varphi \circ \psi)(y),$$

che prova che $\varphi \circ \psi \in \mathrm{End}(G)$. L'applicazione identica id_G è un omomorfismo, quindi $id_G \in \mathrm{End}(G)$, da cui segue che $\mathrm{End}(G)$ è un monoide. □

L'insieme degli elementi invertibili di $\mathrm{End}(G)$ è un gruppo per l'esercizio 4.17.

Definizione 6.23. Il gruppo degli elementi invertibili di $\mathrm{End}(G)$ si chiama il *gruppo degli automorfismi di G* e si denota con $\mathrm{Aut}(G)$. Pertanto

$$\mathrm{Aut}(G) = \{\varphi : G \to G \text{ tale che } \varphi \text{ è un automorfismo}\}$$

e $(\mathrm{Aut}(G), \circ)$ è un gruppo.

Un esempio molto importante di automorfismo di un gruppo G è il *coniugio*.

Definizione 6.24. Siano G un gruppo e $a \in G$. Il *coniugio* è l'applicazione $\varphi_a : G \to G$ definita da $\varphi_a(x) = a^{-1}xa = x^a$ per ogni $x \in G$.

Lemma 6.25. *Siano G un gruppo e $a \in G$. Allora l'applicazione φ_a è un automorfismo per ogni $a \in G$.*

DIMOSTRAZIONE. Si ha:

$$\varphi_a(xy) = a^{-1}(xy)a = (a^{-1}xa)(a^{-1}ya) = \varphi_a(x)\varphi_a(y).$$

Dimostriamo che $\varphi_{a^{-1}}$ è l'inversa di φ_a. Infatti

$$(\varphi_a \circ \varphi_{a^{-1}})(x) = \varphi_a(\varphi_{a^{-1}}(x)) = \varphi_a(axa^{-1}) =$$
$$= a^{-1}(axa^{-1})a = (a^{-1}a)x(aa^{-1}) = x.$$

Quindi $\varphi_a \circ \varphi_{a^{-1}} = \varphi_1 = id_G$. □

L'automorfismo φ_a si chiama anche *automorfismo interno*. Denotiamo con $\mathrm{Inn}(G)$ l'insieme $\{\varphi_a : a \in G\}$ degli automorfismi interni di un gruppo G.

Lemma 6.26. *Sia G un gruppo. Allora* $\mathrm{Inn}(G)$ *è un sottogruppo di* $\mathrm{Aut}(G)$ *e vale*

$$\mathrm{Inn}(G) \cong G/Z(G).$$

DIMOSTRAZIONE. Definiamo l'applicazione $F : G \to \mathrm{Aut}(G)$ tramite

$$F(a) = \varphi_{a^{-1}}.$$

Dimostriamo che F è un omomorfismo, cioè per $a, b \in G$ si ha

$$F(ab) = F(a) \circ F(b), \quad \text{cioè} \quad \varphi_{(ab)^{-1}} = \varphi_{a^{-1}} \circ \varphi_{b^{-1}}.$$

Infatti per ogni $x \in G$ si ha

$$\varphi_{(ab)^{-1}}(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = \varphi_{a^{-1}}(bxb^{-1}) =$$

$$= \varphi_{a^{-1}}(\varphi_{b^{-1}}(x)) = (\varphi_{a^{-1}} \circ \varphi_{b^{-1}})(x).$$

L'immagine di F è per costruzione $\mathrm{Inn}(G)$, che risulta pertanto essere un sottogruppo di $\mathrm{Aut}(G)$ per il lemma 6.8. Calcoliamo il nucleo di F

$$\ker(F) = \{a \in G : \varphi_{a^{-1}} = id_G\},$$

cioè per ogni $x \in G$ si ha $\varphi_{a^{-1}}(x) = x$, da cui $axa^{-1} = x$ e quindi $ax = xa$. Allora $a \in \ker(F)$ se e solo se $a \in Z(G)$. Applicando il primo teorema di omomorfismo 6.13, si ottiene

$$G/\ker(F) \cong \mathrm{Im}(F) \quad \Longrightarrow \quad G/Z(G) \cong \mathrm{Inn}(G),$$

che conclude la dimostrazione. □

Dal lemma 6.26 segue che φ_a risulta essere l'identità se e solo se a è un elemento centrale. Pertanto G è un gruppo abeliano se e solo se φ_a è l'identità per ogni elemento a di G. Nell'esercizio 6.11 si chiede di dimostrare che inoltre $\mathrm{Inn}(G)$ è contenuto nel centro di $\mathrm{Aut}(G)$.

Vogliamo dimostrare che ogni gruppo può essere visto come sottogruppo di un gruppo di permutazioni. Questo significa che dato un qualsiasi gruppo G esiste un omomorfismo iniettivo da G nel gruppo S_X di tutte le permutazioni di un insieme X.

Teorema 6.27. (Teorema di Cayley) *Sia G un gruppo. Allora G è isomorfo ad un sottogruppo di un gruppo di permutazioni.*

DIMOSTRAZIONE. Sia S_G il gruppo delle permutazioni sull'insieme supporto di G. Per ogni $g \in G$, definiamo

$$\mu_g : G \to G \quad \text{con} \quad \mu_g(x) = gx \quad \text{per ogni } x \in G.$$

Dimostriamo che μ_g è una biezione per ogni $g \in G$. Infatti $\mu_g(x) = \mu_g(y)$ se e solo se $gx = gy$, da cui segue per la legge di cancellazione che $x = y$. Inoltre se $y \in G$,

poniamo $x = g^{-1}y$, da cui segue che $\mu_g(x) = gx = y$. Allora μ_g è biettiva ed è pertanto un elemento di S_G. Sia ora $\mu : G \longrightarrow S_G$ definita da $\mu(g) := \mu_g$ per ogni $g \in G$. Dimostriamo che μ è un omomorfismo iniettivo. Siano $g_1, g_2 \in G$, allora $\mu(g_1g_2) = \mu_{g_1g_2}$. Per far vedere che coincide con $\mu_{g_1} \circ \mu_{g_2}$ dimostriamo che queste due permutazioni coincidono su ogni elemento dell'insieme su cui sono definite. Per $x \in G$, vale

$$(\mu_{g_1} \circ \mu_{g_2})(x) = \mu_{g_1}(\mu_{g_2}(x)) = \mu_{g_1}(g_2x) = g_1(g_2x) = (g_1g_2)x = \mu_{g_1g_2}(x).$$

Allora μ è un omomorfismo. Per controllare che μ è iniettivo è pertanto sufficiente calcolare $\ker(\mu) = \{g \in G : \mu(g) = id\}$. Allora $g \in \ker(\mu)$ se e solo se $\mu_g = id$, cioè $\mu_g(x) = gx = x$ per ogni $x \in G$ e quindi $g = 1$. Concludiamo che G è isomorfo a $\mu(G)$, sottogruppo di S_G. □

Nel quinto capitolo abbiamo introdotto rispettivamente nei paragrafi 5.2 e 5.6 i gruppi di permutazioni e i gruppi lineari. Il teorema di Cayley suggerisce l'importanza dei gruppi di permutazioni, in quanto ogni gruppo si può vedere "immerso" in un gruppo di permutazioni. Se il gruppo G è finito, possiamo trovare un'immagine isomorfa a G in un gruppo lineare, come dimostrato nel corollario 6.29. Iniziamo la costruzione di questo omomorfismo. Sia σ una permutazione in S_n, $n \in \mathbb{N}_+$ e sia K un campo. Sia V uno spazio vettoriale su K di dimensione n e $\mathcal{B} = \{v_1, \dots, v_n\}$ una base di V. È noto dalla geometria che l'insieme delle applicazioni lineari da V in se stesso è isomorfo al gruppo delle matrici invertibili $GL_n(K)$. L'isomorfismo viene costruito fissando una base $\mathcal{B}$ di V ed associando ad un'applicazione lineare f di V in sé la matrice che ha come colonne le immagini tramite f dei vettori della base $\mathcal{B}$, espressi come combinazione lineare dei vettori della stessa base $\mathcal{B}$.

Sia f_σ l'applicazione lineare definita sugli elementi di $\mathcal{B}$ da $f_\sigma(v_i) = v_{\sigma(i)}$, per ogni $i = 1, \dots, n$. Denotiamo con A_σ la matrice di f_σ rispetto alla base $\mathcal{B}$. Allora A_σ è una matrice di $GL_n(K)$ tale che in ogni colonna c'è un unico 1 e gli altri elementi sono uguali a 0. Una matrice siffatta si dice *matrice di permutazione*. Proviamo che l'applicazione che manda una permutazione σ nella relativa matrice di permutazione A_σ è effettivamente un omomorfismo, che permette di "rappresentare" il gruppo delle permutazioni su un insieme finito come un sottogruppo di matrici.

Lemma 6.28. *L'applicazione* $f : S_n \longrightarrow GL_n(K)$ *tale che* $f(\sigma) = A_\sigma$ *è un omomorfismo di gruppi.*

DIMOSTRAZIONE. Siano $\sigma, \tau \in S_n$; allora

$$f_{\sigma\circ\tau}(v_i) = v_{\sigma\circ\tau(i)} = v_{\sigma(\tau(i))} = f_\sigma(v_{\tau(i)}) = f_\sigma(f_\tau(v_i)) = (f_\sigma \circ f_\tau)(v_i).$$

Poiché la matrice della composizione $f_\sigma \circ f_\tau$ delle funzioni lineari f_σ e f_τ coincide con il prodotto delle matrici di f_σ e f_τ, possiamo concludere che $A_{\sigma\circ\tau} = A_\sigma A_\tau$. □

Corollario 6.29. *Sia G un gruppo finito. Allora G è isomorfo ad un sottogruppo del gruppo lineare $GL_n(K)$ per un opportuno $n \in \mathbb{N}_+$ e per qualsiasi campo K.*

DIMOSTRAZIONE. È una conseguenza del teorema 6.27 di Cayley e del lemma 6.28, è sufficiente comporre i due omomorfismi ivi descritti. □

Un teorema simile si può dimostrare anche per gruppi infiniti, ma è necessario far ricorso ai gruppi di trasformazioni lineari degli spazi vettoriali di dimensione infinita.

Costruiamo ora un altro omomorfismo di gruppi, sempre legato ai gruppi lineari. Dato il campo K, dalla definizione di campo si deduce che l'insieme $K^* = K \setminus \{0\}$ con il prodotto è un gruppo, che chiamiamo il *gruppo moltiplicativo del campo* K.

Lemma 6.30. *Sia $n \in \mathbb{N}_+$. Allora la funzione determinante* $\det : GL_n(K) \to K^*$ *è un omomorfismo suriettivo di gruppi, il cui nucleo è $SL_n(K)$ e $GL_n(K)/SL_n(K) \cong K^*$.*

DIMOSTRAZIONE. Poiché le matrici in $GL_n(K)$ hanno il determinante non nullo, la funzione det è ben definita. Grazie al teorema di Binet 4.31, si ha

$$\det(AB) = \det(A)\det(B),$$

per ogni $A, B \in GL_n(K)$. Pertanto det è un omomorfismo. Sia $k \in K^*$ e sia $A = (a_{ij})$ la matrice di $GL_n(K)$ con $a_{11} = k$, $a_{ii} = 1$ per ogni $i = 2, \ldots, n$ e $a_{ij} = 0$ per ogni $i, j = 1, \ldots, n$, $i \neq j$. Allora $\det(A) = k$ e quindi det è suriettiva. Ricordando la definizione di $SL_n(K) = \{A \in GL_n(K) : \det(A) = 1\}$ è chiaro che $SL_n(K) = \ker(\det)$. Si conclude applicando il primo teorema di omomorfismo 6.13. □

Consideriamo una trasposizione $\tau = (ij) \in S_n$ e la matrice A_τ. Osserviamo che scambiando la i-esima colonna con la j-esima colonna di A_τ otteniamo la matrice identica I_n e quindi $\det(A_\tau) = -\det(I_n) = -1$. Sia $\sigma \in S_n$; allora σ è un prodotto di trasposizioni, $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$. Pertanto utilizzando i lemmi appena dimostrati,

$$\det(A_\sigma) = \det(A_{\tau_1} A_{\tau_2} \ldots A_{\tau_r}) =$$
$$= \det(A_{\tau_1})\det(A_{\tau_2}) \ldots \det(A_{\tau_r}) = (-1)^r = \operatorname{sgn}(\sigma).$$

Questi semplici fatti permettono di dimostrare il seguente lemma.

Lemma 6.31. *Sia $n \in \mathbb{N}$, $n \geq 2$. La funzione* sgn *da S_n al sottogruppo moltiplicativo $\{-1, 1\}$ di K^* è un omomorfismo suriettivo di gruppi, il cui nucleo è il gruppo alterno A_n, che risulta quindi essere un sottogruppo normale di S_n di indice 2.*

DIMOSTRAZIONE. Il lemma 5.22 prova che $\operatorname{sgn}(f \circ g) = \operatorname{sgn}(f)\operatorname{sgn}(g)$, quindi sgn è un omomorfismo di gruppi da S_n a $\{-1, 1\}$. Inoltre $\operatorname{sgn}(id) = 1$ e $\operatorname{sgn}(\tau) = -1$ se τ è una trasposizione, da cui segue che sgn è suriettivo se $n \geq 2$.

Una dimostrazione alternativa è data dall'osservazione che la funzione sgn è la composizione dell'omomorfismo f definito nel lemma 6.28 con l'omomorfismo det da $GL_n(K)$ a K^*. Per quanto osservato subito prima del lemma, si ha

$$\operatorname{sgn}(\sigma) = \det(A_\sigma) = \det(f(\sigma)) \in \{1, -1\}.$$

Il nucleo dell'applicazione sgn è esattamente il sottogruppo di tutte le permutazioni pari, cioè il gruppo alterno A_n. Allora il gruppo alterno è un sottogruppo normale di S_n e per il primo teorema di omomorfismo 6.13 si ha $S_n/A_n \cong \{-1, 1\}$. □

6.5 Prodotto diretto di gruppi

Nel teorema 4.19 è stato definito il prodotto diretto $H \times K$ di due gruppi H e K ed è stato dimostrato che $H \times K$ è un gruppo con l'operazione definita "componente per componente".

In questo paragrafo analizzeremo meglio la struttura dei prodotti diretti. Mostreremo in particolare che un gruppo G è isomorfo ad un prodotto diretto di due gruppi se e solo se G possiede due sottogruppi normali che generano tutto G e la cui intersezione è identica. Cominciamo dimostrando che le proiezioni, come sono state definite sugli insiemi, sono degli omomorfismi.

Lemma 6.32. *Siano* $p_1 : H \times K \to H$ *e* $p_2 : H \times K \to K$ *le due proiezioni definite da* $p_1((h,k)) = h$ *e* $p_2((h,k)) = k$. *Allora* p_1 *e* p_2 *sono omomorfismi. Inoltre* $\ker p_1 \cong K$ *e* $\ker p_2 \cong H$.

DIMOSTRAZIONE. Se $h, h_1 \in H$ e $k, k_1 \in K$ si ha

$$p_1((h,k)(h_1,k_1)) = p_1((hh_1, kk_1)) = hh_1 = p_1((h,k))p_1((h_1,k_1)).$$

Analogamente si dimostra che p_2 è un omomorfismo. I nuclei $\widetilde{K} = \ker p_1$ e $\widetilde{H} = \ker p_2$ sono sottogruppi normali di $H \times K$. Questo si vede facilmente anche dalla forma esplicita

$$\widetilde{K} = \{(1_H, k) : k \in K\} = \{1_H\} \times K \quad \text{e} \quad \widetilde{H} = \{(h, 1_K) : h \in H\} = H \times \{1_K\}.$$

Infine $i : \widetilde{K} \to K$ e $j : \widetilde{H} \to H$, definiti da $i(1_H, k) = k$ e $j(h, 1_K) = h$ per ogni $h \in H$ e $k \in K$ sono isomorfismi che permettono di identificare i gruppi H e K rispettivamente con i sottogruppi $\widetilde{H}$ e $\widetilde{K}$ del prodotto diretto $H \times K$. □

Dalla dimostrazione del lemma 6.32 segue il corollario 6.33 che permette di scrivere G come prodotto di due suoi sottogruppi normali.

Corollario 6.33. *Sia* $G = H \times K$ *il prodotto diretto di due gruppi* H *e* K. *Allora esistono due sottogruppi normali* $\widetilde{H}$ *e* $\widetilde{K}$ *di* $H \times K$, *isomorfi rispettivamente ad* H *e* K *tali che*

(a) $\widetilde{H} \cap \widetilde{K} = \{1\}$ *e*
(b) $G = \widetilde{H}\widetilde{K}$.

DIMOSTRAZIONE. Basta prendere $\widetilde{K} = \ker p_1$ e $\widetilde{H} = \ker p_2$ come nel lemma 6.32. I sottogruppi $\widetilde{K}$ e $\widetilde{H}$ sono normali perché sono nuclei di omomorfismi. Inoltre (a) è ovvio dalla definizione di $\widetilde{H}$ e $\widetilde{K}$. Per (b) basta notare che se $(h,k) \in H \times K$, allora $(h,k) = (h, 1_K)(1_H, k)$. Possiamo scrivere anche

$$(h,k) = (1_H, k)(h, 1_K)$$

poiché ogni elemento di $\widetilde{H}$ è permutabile con ogni elemento di $\widetilde{K}$. □

Quando non ci saranno ambiguità identificheremo i gruppi H e K con $\widetilde{H}$ e $\widetilde{K}$ rispettivamente.

Vogliamo provare che il corollario 6.33 caratterizza i prodotti diretti di gruppi.

Ricordiamo che in generale il prodotto di due sottogruppi non è un sottogruppo, ma nel caso di sottogruppi normali è ancora un sottogruppo normale, come dimostrato nel lemma 5.69.

Sia G un gruppo che possiede due sottogruppi *normali* H e K che godono delle seguenti due proprietà:

(a) $H \cap K = \{1\}$ e
(b) $G = HK$.

Osserviamo che i due sottogruppi H e K di G sono in particolare dei gruppi. Quindi possiamo considerare il loro prodotto diretto $H \times K$. Dimostreremo nel teorema 6.35 che in questo caso G è isomorfo al prodotto diretto $H \times K$. Per far questo necessitiamo prima di un lemma.

Lemma 6.34. *Siano G un gruppo, H e K due sottogruppi normali di G tali che $H \cap K = \{1\}$. Allora ogni elemento di H commuta con ogni elemento di K.*

DIMOSTRAZIONE. Siano $h \in H$ e $k \in K$. Allora $hkh^{-1} \in K$ per il lemma 5.64 poiché K è normale. Inoltre $k^{-1} \in K$, perciò concludiamo che $hkh^{-1}k^{-1} \in K$. Analogamente, dato che $h^{-1} \in H$ e H è normale, dal lemma 5.64 segue che

$$kh^{-1}k^{-1} \in H.$$

Di conseguenza anche $hkh^{-1}k^{-1} \in H$. Questo dimostra che

$$hkh^{-1}k^{-1} \in K \cap H = \{1\} \implies hkh^{-1}k^{-1} = 1 \implies hk = kh.$$

□

Dimostriamo ora il teorema.

Teorema 6.35. *Siano G un gruppo, H e K due sottogruppi normali di G tali che*

(a) $H \cap K = \{1\}$ e
(b) $G = HK$.

Allora $G \cong H \times K$.

DIMOSTRAZIONE. Definiamo $f : H \times K \to G$ con $f(h, k) = hk$. Per il punto (b) f è un'applicazione suriettiva. Proviamo che f è un omomorfismo. Siano $h, h_1 \in H$ e $k, k_1 \in K$. Allora $h_1 k = k h_1$ per il punto (a) e il lemma 6.34. Quindi

$$f((h,k)(h_1,k_1)) = f((hh_1, kk_1)) = hh_1kk_1 = hkh_1k_1 = f((h,k))f((h_1,k_1)).$$

Per verificare che f è iniettiva basta vedere che $\ker f = \{1\}$. Se $f(h,k) = 1$, allora $hk = 1$ e quindi $h = k^{-1} \in H \cap K$ e per il punto (a) abbiamo $h = k = 1$. Abbiamo così dimostrato che f è un isomorfismo. □

Le condizioni (a) e (b) del teorema 6.35 si ricordano facilmente. Si tende invece a dimenticare l'altra ipotesi essenziale del teorema e cioè che i due sottogruppi H e K devono essere normali. Tale condizione è invece essenziale: se non sono normali, il teorema non è più vero, come dimostreremo nell'esempio 6.39.

Le condizioni richieste nel precedente teorema 6.35 sono in particolare soddisfatte nel caso di un gruppo finito con due sottogruppi normali propri di ordine coprimo.

Teorema 6.36. *Siano G un gruppo, H e K due sottogruppi normali di G tali che $|H| = m$ e $|K| = n$, $m, n \in \mathbb{N}_+$. Supponiamo che*

(a) $(m, n) = 1$ *e*
(b) $|G| = mn$.

Allora $G \cong H \times K$.

DIMOSTRAZIONE. Verifichiamo che $H \cap K = \{1\}$ e $G = HK$.

Poniamo $l = |H \cap K|$. Applicando il teorema di Lagrange 5.52 al gruppo H e al suo sottogruppo $H \cap K$ ricaviamo che l divide m. Analogamente ricaviamo che l divide n. Allora l divide (m, n). Da $(m, n) = 1$ concludiamo che $l = 1$ e quindi $H \cap K = \{1\}$.

Ora poniamo $s = |HK|$. Applicando il teorema di Lagrange al gruppo HK e al suo sottogruppo H ricaviamo che m divide s. Analogamente ricaviamo che n divide s. Allora anche il minimo comune multiplo mn di m ed n divide s. Poiché $s \leq |G| = mn$, concludiamo che $s = mn$ e quindi $HK = G$, da cui per il teorema 6.35 si conclude che $G \cong H \times K$. □

Nel caso dei gruppi abeliani, poiché ogni sottogruppo è normale, le due precedenti condizioni si ridurranno a:

Corollario 6.37. *Sia G un gruppo abeliano e siano H ed K due sottogruppi di G tali che $|H| = m$ e $|K| = n$, $m, n \in \mathbb{N}_+$. Supponiamo che*

(a) $H \cap K = \{1\}$ *oppure* $(m, n) = 1$ *e*
(b) $|G| = mn$.

Allora $G \cong H \times K$.

Vediamo ora alcune applicazioni di quanto appena dimostrato, nel caso di alcuni gruppi abeliani di ordine piccolo.

Esempio 6.38. Sia H il sottogruppo di $\mathbb{Z}_6$ generato da $[2]_6$ e sia K il sottogruppo generato da $[3]_6$. Allora $|K| = 2$ e $|H| = 3$ sono coprimi e $|\mathbb{Z}_6| = 2 \cdot 3$. Per il corollario 6.37 $\mathbb{Z}_6 \cong H \times K$.

Esempio 6.39. Consideriamo il gruppo $G = S_3$ e i suoi due sottogruppi $H = \langle(12)\rangle$ e $K = \langle(123)\rangle$. Allora

(a) $H \cap K = \{1\}$ e
(b) $G = HK$.

Pertanto per il teorema 6.35 $S_3 \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Quindi S_3 è isomorfo ad un gruppo ciclico di ordine 6 e pertanto contiene un elemento di ordine 6. Ma gli elementi di S_3 hanno tutti ordine 1, 2 o 3. Dov'è l'errore?

Le dimostrazioni fatte finora non richiedono nessuna ipotesi sul gruppo G. Iniziamo a "specializzare" il nostro studio per avviarci a studiare i gruppi abeliani finiti. Calcoliamo l'ordine degli elementi di un prodotto $H \times K$ di gruppi H e K in funzione dell'ordine delle loro proiezioni.

Proposizione 6.40. *Siano H e K due gruppi e sia $z = (x, y)$ un elemento del prodotto diretto $H \times K$. Allora l'ordine di z è finito se e solo se sono finiti gli ordini di x e y. In tal caso l'ordine di z è il minimo comune multiplo degli ordini $o(x)$ e $o(y)$.*

DIMOSTRAZIONE. Se $z^m = 1$ per qualche intero m, allora $(x^m, y^m) = (1_H, 1_K)$ e quindi $x^m = 1_H$ e $y^m = 1_K$. Di conseguenza gli ordini di x e y sono finiti qualora sia finito l'ordine di z. Supponiamo adesso che $o(x) = m$ e $o(y) = n$ siano finiti. Dimostreremo che anche $o(z)$ è finito e coincide con il minimo comune multiplo l di m e n. Infatti dall'esercizio 5.1 segue che $o(z)$ divide l. Se $z^s = 1$, allora $x^s = 1_H$ e $y^s = 1_K$, quindi m divide s e n divide s. Di conseguenza anche l divide s e dunque $o(z) = l$. □

Applichiamo la proposizione 6.40 per dimostrare che alcuni prodotti diretti di gruppi non possono essere ciclici.

Esempio 6.41. (a) Il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico. Infatti ogni elemento $x \in \mathbb{Z}_2$ soddisfa $2x = 0$, quindi $\mathbb{Z}_2 \times \mathbb{Z}_2$ non ha elementi di ordine 4.

(b) Sia p un numero primo. Il gruppo $\mathbb{Z}_p \times \mathbb{Z}_p$ non è ciclico. Infatti per la proposizione 6.40 ogni elemento non nullo di $\mathbb{Z}_p \times \mathbb{Z}_p$ ha ordine p, quindi non può generare tutto il gruppo $\mathbb{Z}_p \times \mathbb{Z}_p$.

I gruppi considerati nell'esempio 6.41 stimolano allora una domanda: il prodotto diretto di due gruppi ciclici è ancora ciclico? Il teorema 6.42 fornisce la risposta.

Teorema 6.42. *Siano m e n due numeri naturali, $m, n > 0$. Allora*

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$$

se e solo se m ed n sono coprimi.

DIMOSTRAZIONE. Supponiamo che m ed n siano coprimi. Sia x un generatore di $\mathbb{Z}_m$ e sia y un generatore di $\mathbb{Z}_n$. Allora $o(x) = m$ e $o(y) = n$. Per la proposizione 6.40 l'elemento $z = (x, y)$ di $\mathbb{Z}_m \times \mathbb{Z}_n$ ha ordine $o(z) = mn$. Quindi il sottogruppo ciclico $\langle z \rangle$ di $\mathbb{Z}_m \times \mathbb{Z}_n$ ha mn elementi. Pertanto

$$\mathbb{Z}_{mn} \cong \langle z \rangle = \mathbb{Z}_m \times \mathbb{Z}_n.$$

Ora dimostriamo che se il gruppo $\mathbb{Z}_m \times \mathbb{Z}_n$ è ciclico, allora m e n sono coprimi. Sia $z = (x, y)$ un generatore di $\mathbb{Z}_m \times \mathbb{Z}_n$. Allora

$$mn = o(z) = m.c.m.(o(x), o(y))$$

per la proposizione 6.40. Inoltre per il corollario 5.54, $o(x)$ divide m e $o(y)$ divide n, da cui segue che $o(x) = m$, $o(y) = n$ e $m.c.m.(m, n) = mn$ cioè m ed n sono coprimi. □

Proviamo che l'ordine in cui viene scritto il prodotto diretto di due gruppi non è influente sulla struttura del gruppo.

Lemma 6.43. *Siano H_1 e H_2 due gruppi. Allora $H_1 \times H_2 \cong H_2 \times H_1$.*

DIMOSTRAZIONE. L'applicazione $f : H_1 \times H_2 \to H_2 \times H_1$ definita da $f(x,y) = (y,x)$ per ogni $(x,y) \in H_1 \times H_2$ è un isomorfismo. □

I prodotti diretti si possono definire anche per più di due gruppi. Se H_1, H_2 e H_3 sono tre gruppi, si può definire il prodotto diretto

$$H_1 \times H_2 \times H_3 \quad \text{come} \quad (H_1 \times H_2) \times H_3.$$

Utilizzando lo stesso ragionamento della dimostrazione del lemma 6.43, si può dimostrare che

$$(H_1 \times H_2) \times H_3 \cong H_1 \times (H_2 \times H_3).$$

Quindi questi due gruppi si possono identificare. Un terzo modo per definire il prodotto diretto $H_1 \times H_2 \times H_3$ è quello di introdurre direttamente un'operazione binaria nel prodotto cartesiano $H_1 \times H_2 \times H_3$ ponendo

$$(g_1, g_2, g_3) \cdot (h_1, h_2, h_3) = (g_1h_1, g_2h_2, g_3h_3)$$

per ogni coppia di terne

$$(g_1, g_2, g_3), (h_1, h_2, h_3) \in H_1 \times H_2 \times H_3.$$

Si dimostra facilmente, seguendo la dimostrazione del teorema 4.19, che

$$(H_1 \times H_2 \times H_3, \cdot)$$

risulta un gruppo isomorfo a $(H_1 \times H_2) \times H_3$. In seguito penseremo il prodotto diretto $H_1 \times H_2 \times H_3$ definito nell'ultimo modo.

Dati un insieme non vuoto I e una famiglia di gruppi $\{G_i : i \in I\}$, definiamo nel prodotto cartesiano $\prod_{i \in I} G_i$ un'operazione binaria che lo rende un gruppo.

Lemma 6.44. *Dati un insieme non vuoto I e una famiglia di gruppi $\{G_i : i \in I\}$, sia $G = \prod_{i \in I} G_i$. Per $(g_i)_{i \in I}, (h_i)_{i \in I} \in \prod_{i \in I} G_i$ definiamo il prodotto*

$$(g_i)_{i \in I} \cdot (h_i)_{i \in I} = (g_ih_i)_{i \in I}.$$

Allora $(G, \cdot)$ è un gruppo.

DIMOSTRAZIONE. La dimostrazione è analoga a quella del teorema 4.19. □

Si può dimostrare una caratterizzazione analoga a quella vista nel teorema 6.35 anche per un prodotto diretto finito di gruppi. Bisogna fare attenzione alla condizione (a): si vedano gli esercizi 6.31 e 6.32.

Concludiamo questo paragrafo mostrando alcuni esempi di gruppi abeliani che non possono mai essere prodotti diretti di sottogruppi. Per essere più chiari diamo prima una definizione.

Definizione 6.45. Un sottogruppo non banale H di un gruppo G si dice *addendo diretto* se esiste un altro sottogruppo K di G tale che $G = H \times K$.

Esistono gruppi in cui tutti i sottogruppi non banali sono addendi diretti e gruppi in cui nessun sottogruppo non banale lo è. Diamo un esempio di gruppo in cui nessun sottogruppo non banale è addendo diretto.

Esempio 6.46. Sia p un numero primo e sia $G = \mathbb{Z}_{p^k}$, con $k \geq 2$. Allora ogni sottogruppo proprio di G contiene il sottogruppo non nullo $C = \langle [p^{k-1}]_{p^k} \rangle$. Pertanto la condizione $H \cap K = \{0\}$ non può essere verificata per due sottogruppi propri H e K di G.

Per l'esempio successivo avremo bisogno del seguente lemma che si dimostra applicando il lemma di Zorn.

Lemma 6.47. *Siano H ed L sottogruppi di un gruppo abeliano G con*

$$H \cap L = \{0\}.$$

Allora esiste un sottogruppo M di G contenente L e massimale rispetto alla proprietà di contenere L e di intersecare H banalmente.

DIMOSTRAZIONE. Sia $\mathcal{I} = \{N \leq G : L \leq N \text{ e } H \cap N = \{0\}\}$. Allora $\mathcal{I}$ è un insieme parzialmente ordinato con l'inclusione e non è vuoto perché $L \in \mathcal{I}$. L'insieme $\mathcal{I}$ è un insieme induttivo, in quanto se $\{N_i,\, i \in I\}$ è una catena di elementi di $\mathcal{I}$, l'unione $\bigcup_{i \in I} N_i$ è un sottogruppo di G per il lemma 5.37, contiene L e interseca H banalmente. Allora per il lemma di Zorn esiste un elemento massimale M di $\mathcal{I}$. □

Osserviamo che se G è finito, $\mathcal{I}$ è finito e contiene un elemento massimale e quindi non è necessario utilizzare il lemma di Zorn.

Esempio 6.48. Sia p un numero primo e sia G un gruppo abeliano tale che $px = 0$ per ogni elemento $x \in G$, cioè G ha esponente p. Proviamo che ogni sottogruppo H di G è addendo diretto.

Poiché $H \cap \{0\} = \{0\}$, per il lemma 6.47 esiste un sottogruppo K massimale rispetto alla proprietà $H \cap K = \{0\}$. Verifichiamo che $G = H + K$. Sia $x \in G \setminus K$. Allora il sottogruppo K_1 di G generato da K e da x contiene K propriamente. Quindi per la scelta di K esiste un elemento non nullo $g \in H \cap K_1$. Allora $g = y + mx$, dove $y \in K$ e $m \in \mathbb{Z}$. Poiché $H \cap K = \{0\}$, dobbiamo avere $mx \neq 0$. In altre parole m è coprimo con p e pertanto esiste $m' \in \mathbb{Z}$ tale che $mm' \equiv_p 1$. Allora $m'g = m'y + x$, da cui $x \in H + K$. Per il teorema 6.35 $G \cong H \times K$.

6.6 Esercizi su omomorfismi e prodotti diretti

Esercizio 6.1 Nel gruppo additivo $\mathbb{Q}$ dei numeri razionali si dimostri che il sottoinsieme

$$H = \left\{ \frac{m}{n} \in \mathbb{Q} : m, n \in \mathbb{Z} \text{ e } n \text{ prodotto di primi distinti} \right\}$$

è un sottogruppo di $\mathbb{Q}$. Si determini l'ordine dell'elemento $\frac{5}{36} + H$ in $\mathbb{Q}/H$.

Esercizio 6.2 Sia $G = GL_3(\mathbb{Z})$ definito nell'esercizio 5.35. Assegnati tre interi positivi l, m, n si consideri il sottoinsieme $H_{l,m,n}$ delle matrici della forma

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \quad x \in l\mathbb{Z}, y \in m\mathbb{Z}, z \in n\mathbb{Z}.$$

(a) Si calcoli l'inverso di $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ in G.

(b) Si dimostri che $H_{l,m,n}$ è un sottogruppo di G se e solo se m divide ln.

(c) Si verifichi che l'insieme N di tutte le matrici della forma $\begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ con $y \in 6\mathbb{Z}$ è un sottogruppo normale di $H_{2,6,3}$.

(d) Siano $H = H_{1,1,1}$ e $N = H_{p,p,p}$. Si dimostri che N è un sottogruppo normale di H. Sia $P = H/N$, dimostrare che P è un gruppo non abeliano di ordine p^3.

Esercizio 6.3 Sia H l'insieme delle matrici

$$\begin{pmatrix} 1 & x & y & z \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

con $a, b, x, y, z \in \mathbb{F}_2$.

(a) Si dimostri che H è un sottogruppo del gruppo $GL_4(\mathbb{F}_2)$ e si calcoli l'ordine di H.

(b) Si descriva il centro Z di H.

(c) Si descriva il quoziente H/Z. Si determini, in particolare, se H/Z è ciclico.

Esercizio 6.4 Verificare che la funzione logaritmo con base arbitraria definisce un isomorfismo tra i gruppi $(\mathbb{R}_+, \cdot)$ e $(\mathbb{R}, +)$.

Esercizio 6.5 Si consideri l'applicazione $\tau : GL_2(\mathbb{R}) \to GL_2(\mathbb{R})$ che manda ogni matrice A nella sua trasposta A^t, cioè

$$\tau\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}.$$

L'applicazione τ così definita è un omomorfismo?

Esercizio 6.6 Dimostrare che:

(a) il gruppo quoziente $(\mathbb{R}/\mathbb{Z}, +)$ è isomorfo al gruppo $(\mathbb{S}, \cdot)$, se $\mathbb{S}$ è l'insieme dei numeri complessi z con $|z| = 1$;
(b) l'insieme $(\mathbb{U}_n, \cdot)$ delle radici n-esime dell'unità $n > 1$ è un sottogruppo di $\mathbb{S}$;
(c) il gruppo quoziente $(\mathbb{Z}/n\mathbb{Z}, +)$ è isomorfo al gruppo $(\mathbb{U}_n, \cdot)$.

Esercizio 6.7 Provare che i gruppi $(\mathbb{Q}, +)$ e $(\mathbb{Q} \setminus \{0\}, \cdot)$ non sono isomorfi.

Esercizio 6.8 Sia G un gruppo e sia X un insieme di generatori di G. Se per una coppia di omomorfismi $f, g : G \to H$ si ha $f(x) = g(x)$ per ogni $x \in X$, si dimostri che $f = g$.

Esercizio 6.9 Siano G un gruppo, F un sottoinsieme di $G \times G$ e $f : G \to G$ una funzione tale che $f(xy) = f(x)f(y)$ per ogni $(x, y) \in (G \times G) \setminus F$. Si provi che f è un omomorfismo di G nei seguenti casi:
(a) F finito, G infinito;
(b) F e G finiti con $|F| < 1/3|G|$;
(c) G infinito e $|F| < |G|$ (per esempio, F numerabile, mentre G non numerabile).

Esercizio 6.10 Sia $\mathbb{F}_p$ il campo con p elementi, p primo. Si calcoli $|SL_n(\mathbb{F}_p)|$per $n \in \mathbb{N}_+$.

Esercizio 6.11 Sia G un gruppo. Si dimostri che $\mathrm{Inn}(G)$ è un contenuto nel centro di $\mathrm{Aut}(G)$.

Esercizio 6.12 Siano H e K due gruppi. Dimostrare che $H \times K$ è abeliano se e solo se H e K sono abeliani.

Esercizio 6.13 Sia G un gruppo e sia $D = \{(g, g) : g \in G\}$ il sottogruppo diagonale del prodotto diretto $G \times G$. Dimostrare che D è un sottogruppo normale di $G \times G$ se e solo se G è abeliano.

Esercizio 6.14 Nel prodotto diretto $H \times K$ si definiscano i sottogruppi $\overline{H} = H \times \{1\}$ e $\overline{K} = \{1\} \times K$. Se A è un sottogruppo di $H \times K$ contenente $\overline{H}$, si dimostri che

$$A \cong \overline{H} \times (A \cap \overline{K}).$$

Esercizio 6.15 Siano G un gruppo, H e K sottogruppi normali di G con

$$H \cap K = \{1\} \text{ e } G = HK,$$

da cui $G \cong H \times K$. Provare che:

(a) $Z(G) = Z(H)Z(K)$;
(b) se $N \trianglelefteq G$ e $N \not\subseteq Z(G)$ provare che $H \cap N \neq \{1\}$ oppure $K \cap N \neq \{1\}$;
(c) se H e K sono semplici e non abeliani, dimostrare che H e K sono gli unici sottogruppi normali non banali di G.

Esercizio 6.16 Si consideri il gruppo $G = \{(a, b, c,)|a, b, c \in \mathbb{Z}\}$ con il prodotto definito dalla posizione

$$(a, b, c) \cdot (a', b', c') = (a + a', b + b' + ac', c + c').$$

(a) Si determinino l'identità e l'inverso dell'elemento (a, b, c).
(b) Sia $f : G \to \mathbb{Z} \times \mathbb{Z}$ definito da $f((a, b, c)) = (a, c)$. Si verifichi che f è un omomorfismo e si determini $\ker f$.
(c) Si verifichi che $\ker(f)$ coincide con il centro $Z(G)$ di G.

Esercizio 6.17 Siano $f : H \to H_1$ e $t : K \to K_1$ due omomorfismi. Sia

$$F : H \times K \to H_1 \times K_1 \text{ l'applicazione definita da } F(g, h) = (f(g), t(h)).$$

Dimostrare che:

(a) F è un omomorfismo;
(b) F è iniettivo se e solo se lo sono f e t;
(c) F è suriettivo se e solo se lo sono f e t;
(d) F è un isomorfismo se e solo se lo sono f e t.

Esercizio 6.18 Sia G un gruppo abeliano e siano H e K sottogruppi di G. Dimostrare che:

(a) il sottoinsieme $H + K = \{h + k : h \in H, k \in K\}$ di G è un sottogruppo;
(b) il sottogruppo $H + K$ è isomorfo ad un quoziente del prodotto diretto $H \times K$ e quindi $|H + K|$ divide $|H| \cdot |K|$ nel caso in cui H e K siano finiti;
(c) se gli ordini $|H|$ e $|K|$ sono coprimi, provare che

$$H + K \cong H \times K \quad \text{e pertanto} \quad |H + K| = |H| \cdot |K|.$$

Esercizio 6.19 Sia G un gruppo abeliano non ciclico di ordine 9. Dimostrare che $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Esercizio 6.20 Siano p e q due numeri primi distinti. Si trovi il numero dei sottogruppi del gruppo $G = \mathbb{Z}_p \times \mathbb{Z}_q$.

Esercizio 6.21 Sia p un numero primo. Si trovi il numero dei sottogruppi del gruppo $\mathbb{Z}_p \times \mathbb{Z}_p$.

Esercizio 6.22 Dimostrare che il gruppo simmetrico S_3 non è prodotto diretto di due suoi sottogruppi propri.

Esercizio 6.23 Siano G ed H gruppi finiti e $f : G \to H$ un omomorfismo. Si dimostri che:

(a) per ogni $g \in G$ si ha che $o(f(g))$ divide $o(g)$;
(b) se $o(f(g)) = o(g)$ per ogni $g \in G$, allora f è iniettivo;
(c) se f è suriettivo, allora $|H|$ divide $|G|$;
(d) se f è iniettivo, allora $|G|$ divide $|H|$.

Esercizio 6.24 Siano G un gruppo abeliano e $f : G \to G$ un omomorfismo di gruppi tale che $f \circ f = f$. Dimostrare che

$$G \cong f(G) \times \ker f.$$

Esercizio 6.25 Siano $f : K \to G$ e $t : K \to H$ due omomorfismi. Sia

$$F : K \to G \times H \quad \text{l'applicazione definita da} \quad F(x) = (f(x), t(x)).$$

Dimostare che:

(a) F è un omomorfismo e $p_1 \circ F = f$, $p_2 \circ F = t$;
(b) ogni omomorfismo $s : K \to G \times H$ si ottiene in questo modo cioè gli omomorfismi $f : K \to G$ e $t : K \to H$ dati da $f = p_1 \circ s$ e $t = p_2 \circ s$ danno luogo ad un omomorfismo $F : K \to G \times H$ come sopra descritto, che coincide con s.

Esercizio 6.26 Sia $n > 2$ un numero intero e siano

$$f_1 : G \to H_1, \quad f_2 : G \to H_2, \quad \dots, \quad f_n : G \to H_n$$

omomorfismi. Si provi che esiste un unico omomorfismo

$$f : G \to H_1 \times H_2 \times \ldots \times H_n$$

tale che $p_i \circ f = f_i$, dove

$$p_i : H_1 \times \ldots \times H_n \to H_i,$$

per $i = 1, \ldots, n$ sono le proiezioni. Inoltre ogni omomorfismo

$$f : G \to H_1 \times H_2 \times \ldots \times H_n$$

ha questa forma.

Esercizio 6.27 Sia G il sottogruppo additivo dei numeri complessi

$$G = \{x + iy | x, y \in \mathbb{Z}\}.$$

(a) Si provi che l'applicazione $f : G \to G$ definita da $f(x + iy) = x + y$ è un endomorfismo di G;
(b) si dimostri che $\ker f$ è ciclico e se ne trovi un generatore;
(c) si trovi $f(G)$.

Esercizio 6.28 Sull'insieme $G = \mathbb{Z}_4 \times \{-1, 1\}$ si definisca un'operazione $\cdot$ ponendo per ogni $(x, u), (y, v) \in G$,

$$(x, u) \cdot (y, v) = (x + uy, uv).$$

(a) Si dimostri che G con questa operazione è un gruppo non abeliano.
(b) Si trovi un sottogruppo di G che non è normale.

(c) * Si dimostri che G è isomorfo al gruppo diedrale D_8 definito nell'esercizio 5.51.

Esercizio 6.29 In $G = GL_2(\mathbb{R})$ si consideri il coniugio tramite la matrice

$$\eta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R}).$$

Si calcoli l'immagine tramite φ_η dei seguenti sottogruppi:

$$T_2^+ = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\};$$

$$T_2^- = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\};$$

$$D_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} : a, c \in \mathbb{R}, ac \neq 0 \right\}.$$

Esercizio 6.30 Dati un insieme non vuoto I e una famiglia di gruppi $\{G_i : i \in I\}$, si consideri il gruppo $G = \prod_{i \in I} G_i$, definito nel lemma 6.44. Sia $I = J \cup L$ una partizione non banale di I. Se $G_J = \prod_{i \in J} G_i$ e $G_L = \prod_{i \in L} G_i$, si dimostri che $G \cong G_J \times G_L$.

Esercizio 6.31 Sia $r \in \mathbb{N}, r \geq 2$. Siano G un gruppo ed $N_1, \ldots, N_r$ sottogruppi normali di G. Denotiamo con H_i il prodotto dei sottogruppi N_j, per $j = 1, 2, \ldots, r$, $j \neq i$. Se

(a) $N_i \cap H_i = \{1\}$ per ogni $i = 1, \ldots, r$ e
(b) $G = N_1 \ldots N_r$,

allora $G \cong N_1 \times \ldots \times N_r$.

Esercizio 6.32 * Siano G gruppo ed $N_1, \ldots, N_r$ sottogruppi normali di G, tali che

(a) $N_i \cap N_j = \{1\}$ per ogni $i, j = 1, \ldots, r, i \neq j$ e
(b) $G = N_1 \ldots N_r$.

Si dica se $G \cong N_1 \times \ldots \times N_r$.

Esercizio 6.33 Sull'insieme $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ si definisca un'operazione $\cdot$ ponendo per ogni $(x, y, z), (u, v, w) \in G$

$$(x, y, z) \cdot (u, v, w) = (x + (-1)^z u, y + v, z + w).$$

(a) Si dimostri che G con questa operazione è un gruppo non abeliano.
(b) Si dimostri che il sottoinsieme $N = \mathbb{Z} \times \{0\} \times \{0\}$ di G è un sottogruppo normale di G e che G/N è isomorfo al gruppo $\mathbb{Z} \times \mathbb{Z}$.
(c) Esistono sottogruppi di G che non sono normali?
(d) Calcolare il centro di G.

Esercizio 6.34 Sia G l'insieme dei numeri complessi del tipo $a + ib$ con $a, b \in \mathbb{Q}$ non entrambi nulli;

(a) si provi che G è un gruppo rispetto alla moltiplicazione;
(b) si calcoli il periodo di $1 + i$, $1/2i$ e -1;
(c) si provi che l'applicazione $f : G \to G$ definita da $f : z \mapsto z^{-2}$ per ogni $z \in G$ è un endomorfismo di G non suriettivo.

Esercizio 6.35 Sia N il sottogruppo ciclico di $(\mathbb{R}^*, \cdot)$ generato da π.

(a) Quanti elementi di ordine 2 ha il gruppo quoziente $\mathbb{R}^*/N$?
(b) Si determinino gli elementi di ordine finito del quoziente $\mathbb{R}^*/N$.

Esercizio 6.36 * Dimostrare che il sottogruppo $\mathbb{Q}$ del gruppo additivo $(\mathbb{R}, +)$ è addendo diretto di $\mathbb{R}$.

Esercizio 6.37 * Sia G sottogruppo del gruppo additivo $(\mathbb{R}, +)$. Dimostare che G è addendo diretto di $\mathbb{R}$ se e solo se $\mathbb{R}/G$ non ha elementi periodici.

Esercizio 6.38 Sia p un primo e sia G il sottoinsieme di $\mathbb{C}$ delle radici p^n-esime dell'unità al variare di $n \in \mathbb{N}$. Dimostrare che:

(a) $(G, \cdot)$ è un sottogruppo infinito di $(\mathbb{C}, \cdot)$;
(b) ogni sottogruppo proprio di G è ciclico finito;
(c) G è isomorfo al gruppo quoziente $\mathbb{Q}_p/\mathbb{Z}$, dove $\mathbb{Q}_p$ è il sottogruppo di $\mathbb{Q}$ formato di tutte le frazioni del tipo a/p^n al variare di $a, n \in \mathbb{Z}$.

Esercizio 6.39 (a) Dimostrare che se $f : G \to G_1$ è un isomorfismo di gruppi e $H \leq G$, allora $G/H \cong G_1/f(H)$.
(b) Sia G il gruppo $(\mathbb{R}^*, \cdot)$. Sia $g \in G \setminus \{\pm 1\}$. Dimostrare che $\langle g \rangle \cong \mathbb{Z}$.
(c) Siano $g, h \in G \setminus \{\pm 1\}$, dimostrare che $G/\langle g \rangle \cong G/\langle h \rangle$.

Esercizio 6.40 Dimostrare che $(\mathbb{R}^*, \cdot)$ è isomorfo a $\mathbb{Z}_2 \times (\mathbb{R}, +)$.

Esercizio 6.41 Calcolare quanti sono gli elementi di periodo n in $\mathbb{R}/\mathbb{Z}$.

7

Gruppi abeliani

In questo capitolo studiamo i gruppi abeliani con lo scopo di "classificare" i gruppi abeliani con qualche proprietà particolare, per esempio: i gruppi abeliani ciclici nel teorema 7.1, i gruppi abeliani finiti nel teorema 7.16 e i gruppi abeliani cociclici nel teorema 7.23. Quando in teoria dei gruppi si usa la parola "classificare" si intende trovare tutti i gruppi, a meno di isomorfismo, con una certa proprietà. Quindi, dato un qualunque gruppo abeliano G con le proprietà richieste, dimostriamo che in realtà G è isomorfo ad un gruppo che già conosciamo. Per esempio, nel caso specifico dei gruppi ciclici si dimostra nel primo paragrafo che un gruppo ciclico G deve essere isomorfo a $\mathbb{Z}$ oppure a $\mathbb{Z}_m$, nel caso in cui G sia finito di cardinalità m. Studiamo anche i generatori dei gruppi ciclici e infine ne determiniamo la "struttura", cioè descriviamo tutti i suoi sottogruppi, i suoi sottogruppi normali e i suoi quozienti. In generale non è facile determinare la struttura di un gruppo, ma nel caso dei gruppi ciclici, questa viene determinata completamente. Analogamente, si dimostra nel secondo paragrafo che ogni gruppo abeliano finito è isomorfo an un prodotto diretto di gruppi ciclici. Il terzo paragrafo è dedicato ai gruppi abeliani infiniti, con particolare enfasi ai sottogruppi di $\mathbb{Q}$ e ai gruppi cociclici.

7.1 Gruppi ciclici

Nella dimostrazione del seguente teorema sarà determinante l'utilizzo del primo teorema di omomorfismo e la conoscenza dei sottogruppi dei numeri interi $(\mathbb{Z}, +)$.

Teorema 7.1. *Sia $(G, \cdot)$ un gruppo ciclico. Allora:*

(a) $G \cong \mathbb{Z}$, se G è infinito; oppure
(b) G è isomorfo a $\mathbb{Z}_m$ per qualche $m \in \mathbb{N}_+$ se G è finito con m elementi.

DIMOSTRAZIONE. Sia x un generatore di G. Allora l'applicazione $f : \mathbb{Z} \to G$ definita da $f(n) = x^n$ per ogni $n \in \mathbb{Z}$ è suriettiva. Dal lemma 5.2 segue che f è un omomorfismo, pertanto il suo nucleo $\ker f$ è un sottogruppo di $\mathbb{Z}$. Per il lemma 5.33 esiste $m \geq 0$ tale che $\ker f = m\mathbb{Z}$. Consideriamo due casi:

(a) se $m = 0$, allora $\ker f = \{0\}$, cioè f è iniettiva, quindi f è un isomorfismo e $G \cong \mathbb{Z}$;

(b) Se $m > 0$, allora per il primo teorema di omomorfismo $G \cong \mathbb{Z}/\ker f = \mathbb{Z}_m$.
□

Studiamo la struttura di un gruppo ciclico e cominciamo a capire quanti possono essere i generatori di un gruppo ciclico.

Lemma 7.2. *(a) $\mathbb{Z}$ ha due generatori.*
(b) $\mathbb{Z}_m$ ha $\varphi(m)$ generatori, per $m \in \mathbb{N}_+$.

DIMOSTRAZIONE. (a) Gli elementi ± 1 sono generatori di $\mathbb{Z}$. Se a è un generatore di $\mathbb{Z}$, allora $\langle a \rangle = a\mathbb{Z} = \mathbb{Z}$. Questo è possibile se e solo se $a = \pm 1$.

(b) Per vedere che $\mathbb{Z}_m$ ha $\varphi(m)$ generatori, basta notare che per un generatore a di $\mathbb{Z}_m$ un multiplo ka risulta generatore se e solo se k è coprimo con m, per (c) del lemma 5.5. Quindi i generatori di $\mathbb{Z}_m$ corrispondono ai numeri interi k che soddisfano $0 \leq k < m$ e sono coprimi con m. □

Siamo in grado di dimostrare che sottogruppi e quozienti di gruppi ciclici sono ciclici.

Proposizione 7.3. *Sia C un gruppo ciclico. Allora:*

(a) ogni quoziente di C è ciclico;
(b) ogni sottogruppo di C è ciclico.

DIMOSTRAZIONE. (a) Sia $H = C/N$ un quoziente di C, dove N un sottogruppo di C necessariamente normale poiché C è abeliano. Allora l'omomorfismo canonico $\pi : C \to C/N$ è suriettivo e per il lemma 6.7 (b) C/N è ciclico.

(b) Sia $C = \langle g \rangle$ e sia $f : \mathbb{Z} \to C$ l'omomorfismo suriettivo definito da $f(1) = g$. Allora per ogni $L \leq C$, si ha $L = f(f^{-1}(L))$. Per il lemma 5.33 il sottogruppo $f^{-1}(L)$ di $\mathbb{Z}$ è ciclico e quindi, per il lemma 6.7 (b) anche L risulta ciclico. □

Come già accennato, non è detto che per ogni divisore d di $|G|$ esista un sottogruppo di ordine d. Infatti nel gruppo alterno A_4 non ci sono sottogruppi di ordine 6, come si chiede di dimostrare nell'esercizio 8.21. Nei gruppi ciclici invece ogni divisore dell'ordine di $|G|$ risulta essere l'ordine di un unico sottogruppo di G.

Teorema 7.4. *Sia C un gruppo ciclico finito. Allora per ogni divisore d di $m = |C|$ esiste un unico sottogruppo di C di ordine d.*

DIMOSTRAZIONE. Sia x un generatore di C. Allora per $m_1 = m/d$ l'elemento $y = x^{m_1}$ ha ordine d e pertanto il sottogruppo $\langle y \rangle$ ha ordine d. Siano H un sottogruppo di C di ordine d e z un generatore di H. Allora $o(z) = d$ ed esiste un unico $k \in N_+$, $k \leq m$ tale che $z = x^k$. Poiché $d = m/(k, m)$, concludiamo che $(k, m) = m_1$, quindi $k = m_1 k_1$, con $(k_1, d) = 1$. Si ha $z = x^k = x^{m_1 k_1} = y^{k_1} \in \langle y \rangle$, da cui $H \leq \langle y \rangle$. Poiché $|H| = |\langle y \rangle|$, si conclude $H = \langle y \rangle$. □

Il teorema 7.4 stabilisce una biezione tra i sottogruppi di un gruppo ciclico finito G e i divisori di $|G|$. Per completare lo studio dei gruppi ciclici finiti, analizziamo

il loro gruppo degli automorfismi. Dall'esempio 4.17 sappiamo che $(\mathbb{Z}_m, \cdot)$ è un monoide, allora per l'esercizio 4.17 l'insieme $U(\mathbb{Z}_m) = \{[k]_m : \text{ con } (k, m) = 1\}$ è un gruppo. Dalla definizione della funzione di Eulero $\varphi(m)$, sappiamo che $U(\mathbb{Z}_m)$ ha cardinalità $\varphi(m)$. Vediamone qualche esempio.

Esempio 7.5. Descriviamo il gruppo $G = (U(\mathbb{Z}_8), \cdot)$. Poiché $\varphi(8) = 4$, G ha quattro elementi; più precisamente

$$G = \{[1]_8, [3]_8, [5]_8, [7]_8\}.$$

Osserviamo che

$$[3]_8^2 = [5]_8^2 = [7]_8^2 = [1]_8.$$

Pertanto

$$o([3]_8) = o([5]_8) = o([7]_8) = 2.$$

Allora i sottogruppi $H = \langle [3]_8 \rangle$ e $K = \langle [5]_8 \rangle$ hanno entrambi due elementi e

$$H \cap K = \{[1]_8\}.$$

Per il corollario 6.37 $G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, essendo $H \cong K \cong \mathbb{Z}_2$.

Questa descrizione produce esplicitamente i sottogruppi H e K per i quali risulta $G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Il gruppo degli elementi invertibili di $\mathbb{Z}_m$ è collegato al suo gruppo degli automorfismi.

Teorema 7.6. *Sia* $m > 1$ *un numero intero. Allora* $\mathrm{Aut}(\mathbb{Z}_m) \cong (U(\mathbb{Z}_m), \cdot)$.

DIMOSTRAZIONE. L'elemento $[1]_m$ è un generatore del gruppo ciclico $\mathbb{Z}_m$, cioè

$$\mathbb{Z}_m = \langle [1]_m \rangle.$$

Allora ogni elemento di $\mathbb{Z}_m$ è del tipo $k[1]_m$ con $k \in \mathbb{Z}$. Sia $f \in \mathrm{Aut}(\mathbb{Z}_m)$. Posto $a = f([1]_m)$, avremo quindi

$$f(s[1]_m) = sa \quad \text{per ogni} \quad s \in \mathbb{Z}.$$

In altre parole $a = f([1]_m)$ determina univocamente f. Sia $a = k[1]_m$, con $0 \le k < m$. Poiché $f([1]_m)$ è un generatore di $\mathbb{Z}_m$ per il lemma 6.7 (a) si ha $o(a) = m$ e quindi $(k, m) = 1$. Poniamo $\Phi(f) = f([1]_m)$. Abbiamo così definito un'applicazione

$$\Phi : \mathrm{Aut}(\mathbb{Z}_m) \to U(\mathbb{Z}_m).$$

Dimostriamo che Φ è un omomorfismo. Per $f, g \in \mathrm{Aut}(\mathbb{Z}_m)$ con $f([1]_m) = [n]_m$ e $g([1]_m) = [k]_m$ si ha

$$\Phi(f \circ g) = (f \circ g)([1]_m) = f(g([1]_m)) = f([k]_m) =$$

$$f(k[1]_m) = kf([1]_m) = k[n]_m = [kn]_m = [k]_m[n]_m = \Phi(f)\Phi(g).$$

Sia $f \in \ker(\Phi)$; allora $\Phi(f) = f([1]_m) = [1]_m$, cioè f è l'identità di $\mathbb{Z}_m$, da cui segue che Φ è iniettiva.

Per vedere che Φ è suriettiva definiamo per ogni intero n un'applicazione ψ_n da $\mathbb{Z}_m$ in sé con

$$\psi_n([k]_m) = [nk]_m = n[k]_m$$

per ogni $[k]_m \in \mathbb{Z}_m$. Si vede facilmente che ψ_n è un omomorfismo da $\mathbb{Z}_m$ in se stesso. Se $(n, m) = 1$, allora ψ_n è iniettiva, poiché $nt \equiv_m 0$ implica $t \equiv_m 0$ per ogni $t \in \mathbb{Z}$. Essendo $\mathbb{Z}_m$ finito, ψ_n è un automorfismo per ogni n coprimo con m. Sia $[n]_m \in U(\mathbb{Z}_m)$; allora

$$\Phi(\psi_n[1]_m) = [n]_m,$$

cioè Φ è suriettiva. □

7.2 Gruppi abeliani finiti

In questa sezione vogliamo dimostrare il teorema 7.16 di struttura dei gruppi abeliani finiti.

Esempio 7.7. Applicando due volte il teorema 6.42 è facile dimostrare che $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Più in generale, se m, n e k sono numeri interi positivi a due a due coprimi, allora $\mathbb{Z}_{kmn} \cong \mathbb{Z}_k \times \mathbb{Z}_m \times \mathbb{Z}_n$.

Questa decomposizione di un gruppo ciclico in prodotto diretto di gruppi ciclici di ordini coprimi è un caso particolare di un procedimento che si può applicare più in generale ad un gruppo abeliano finito. Il seguente teorema infatti descrive la struttura dei gruppi abeliani finiti.

Teorema di Frobenius-Stickelberger. *Ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici.*

Ci serviranno diversi lemmi sulle proprietà riguardanti i gruppi abeliani. Dapprima esaminiamo alcuni casi di gruppi "piccoli". Abbiamo provato nel lemma 5.60 che i gruppi di ordine p sono ciclici. Pertanto, a meno di isomorfismi, esiste un unico gruppo di ordine un primo p.

Vediamo ora i gruppi in cui tutti gli elementi hanno ordine 2.

Lemma 7.8. *Sia G un gruppo tale che tutti i suoi elementi diversi da 1 hanno periodo 2. Allora G è abeliano.*

DIMOSTRAZIONE. Siano $x, y \in G$. Allora $x^2 = y^2 = (xy)^2 = 1$. Pertanto

$$x = x^{-1}, \quad y = y^{-1} \text{ e } xy = (xy)^{-1}.$$

Ma $(xy)^{-1} = y^{-1}x^{-1} = yx$, da cui $xy = yx$. □

Osserviamo che se G è un gruppo in cui tutti gli elementi diversi da 1 hanno ordine 2 (e quindi abeliano per quanto appena dimostrato), questo significa che $2x =$

0 per ogni $x \in G$. Pertanto l'applicazione $\varphi : \mathbb{F}_2 \times G \to G$, data da $\varphi(a, x) = ax$, per ogni $a \in \mathbb{F}_2, x \in G$ è ben definita e rende il gruppo abeliano G uno spazio vettoriale su $\mathbb{F}_2$. Pertanto se $|G|$ è finito, esiste $n \in \mathbb{N}_+$ tale che $G \cong \mathbb{F}_2^n$.

Poiché 4 è il più piccolo numero naturale che non è un primo, studiamo ora i gruppi di ordine 4.

Lemma 7.9. *Sia G un gruppo di ordine 4; allora $G \cong \mathbb{Z}_4$ o $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

DIMOSTRAZIONE. Se G ha un elemento di ordine 4, allora G è ciclico e pertanto $G \cong \mathbb{Z}_4$. Possiamo supporre che tutti gli elementi di G diversi da 1 abbiano periodo 2. Per il lemma 7.8 il gruppo G è abeliano. Si scelga un elemento non nullo $a \in G$; il sottogruppo $H = \langle a \rangle$ ha due elementi. Sia $b \in G \setminus H$; allora $K = \langle b \rangle$ ha due elementi e $K \not\subseteq H$, quindi $H \cap K = \{1\}$ e HK contiene propriamente K, da cui $HK = G$. Ora si applica il corollario 6.37. □

La dimostrazione del lemma 7.9 si poteva facilmente concludere utilizzando l'osservazione precedente il lemma stesso che se $|G| = 4$ e ogni elemento ha ordine 2, allora $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

È relativamente facile descrivere tutti i gruppi abeliani di ordine minore o uguale a 15 senza far ricorso al teorema di struttura 7.16, come verrà chiesto di fare nell'esercizio 7.1.

Iniziamo ora la dimostrazione del teorema di Frobenius-Stickelberger.

Lemma 7.10. *Siano G un gruppo, H un sottogruppo di G ed $a \in G$. Se esistono due interi coprimi m ed n tali che $ma \in H$ e $na \in H$, allora $a \in H$.*

DIMOSTRAZIONE. Siano $u, v \in \mathbb{Z}$ tali che $1 = um + vn$. Allora

$$a = u(ma) + v(na) \in H.$$

□

Si osservi che il lemma 7.10 qui enunciato in notazione additiva vale anche se il gruppo G non è abeliano.

Abbiamo visto nel corollario 5.54 del teorema di Lagrange che l'ordine di un elemento divide sempre l'ordine del gruppo e abbiamo anche visto che non sempre, dato un divisore dell'ordine del gruppo, esiste un sottogruppo di quell'ordine. Ci sono però alcuni casi particolari in cui ciò accade. È il caso di un divisore primo dell'ordine del gruppo. Il seguente lemma, noto come lemma di Cauchy, vale per tutti i gruppi finiti, ma per ora lo dimostriamo solo nel caso abeliano.

Lemma 7.11. (Lemma di Cauchy nel caso abeliano) *Sia p un numero primo e G un gruppo abeliano finito tale che p divide $|G|$. Allora G ha elementi di ordine p.*

DIMOSTRAZIONE. L'asserto segue dal teorema 7.4 se G è ciclico. Scriviamo

$$m = |G| = pn$$

e procediamo per induzione su n. Per $n = 1$ ogni elemento non nullo di G ha ordine p. Supponiamo $n > 1$. Sia $a \in G$ un elemento non nullo. Se p divide l'ordine k di $H = \langle a \rangle$, si applica l'osservazione iniziale per trovare un elemento di ordine p di H. Supponiamo che p non divida k. Consideriamo il gruppo quoziente $G_1 = G/H$ e l'omomorfismo canonico $\pi : G \to G_1$. Ora $m_1 = |G_1| = m/k < m$ e $p | m_1$ poiché p divide $m = m_1 k$ e $(p, k) = 1$. Per l'ipotesi induttiva esiste $y \in G_1$ di ordine p. Sia $x \in G$ con $\pi(x) = y$. Se $K = \langle x \rangle$ si ha che $\pi(K) = \langle y \rangle$. In altre parole la restrizione di π a K dà luogo ad un omomorfismo suriettivo $K \to \langle y \rangle$. Dunque $p = o(y) = |\langle y \rangle|$ divide $s = |K|$ per il corollario 6.15.

Allora il sottogruppo ciclico K contiene un elemento di ordine p per il teorema 7.4. □

Il seguente lemma serve per la dimostrazione della proposizione successiva.

Lemma 7.12. *Sia* $(G, +)$ *un gruppo abeliano finito e sia* m *un intero positivo tale che* $mx = 0$ *per ogni* $x \in G$. *Allora* $|G|$ *divide qualche potenza di* m.

DIMOSTRAZIONE. Sia p un primo che divide $|G|$; allora esiste $x \in G$ di ordine p per il lemma 7.11 di Cauchy nel caso abeliano. Da $mx = 0$ e dal lemma 5.5 deduciamo che p divide m.

Abbiamo così dimostrato che ogni numero primo che divide $|G|$ divide anche m. Per il teorema fondamentale dell'aritmetica questo implica che $|G|$ divide qualche potenza opportuna di m. □

Siamo ora giunti alla parte cruciale della dimostrazione. La proposizione 7.13 e il successivo teorema 7.14 garantiscono che se G è un gruppo abeliano di ordine finito $n = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$, con $a_i \in \mathbb{N}$, p_i primo per ogni $i = 1, \dots, t$ e $p_i \neq p_j$ se $i \neq j$, allora G si può scrivere come prodotto diretto di t gruppi $P_1, \dots, P_t$ di ordini rispettivamente $p_1^{a_1}, p_2^{a_2}, \dots, p_t^{a_t}$.

Proposizione 7.13. *Siano* m *ed* n *due numeri interi positivi coprimi e* G *un gruppo abeliano di ordine* mn. *Allora:*

(a) $H = \{x \in G : nx = 0\}$ *è un sottogruppo di* G *di ordine* n*;*
(b) $K = \{x \in G : mx = 0\}$ *è un sottogruppo di* G *di ordine* m*;*
(c) $G \cong H \times K$.

DIMOSTRAZIONE. (a), (b) Se $nx = 0$ e $ny = 0$ per $x, y \in G$, allora anche

$$n(x - y) = nx - ny = 0.$$

Poiché anche $0 \in H$, si conclude che H è un sottogruppo di G. Analogamente si prova che $K \leq G$.

(c) Per provare che $G \cong H \times K$ proviamo che $H \cap K = \{0\}$. Infatti, se $x \in H \cap K$, allora $nx = 0$ e $mx = 0$. Essendo m ed n coprimi, si deduce dal lemma 7.10 che $x = 0$.

Per verificare che $G = H + K$ prendiamo $y \in G$. Essendo m ed n coprimi esistono $u, v \in \mathbb{Z}$ tali che $1 = um + vn$. Allora avremo $y = u(my) + v(ny)$ e

$n(my) = (nm)y = 0$, poiché $|G| = nm$. Quindi $my \in H$; analogamente $ny \in K$ e $y \in H + K$. Per il teorema 6.35 si conclude che $G \cong H \times K$.

Per il lemma 7.12 $|H|$ divide qualche potenza di n, e pertanto $|H|$ è coprimo con m. D'altra parte, essendo H un sottogruppo di G, $|H|$ divide $|G| = mn$. Quindi $|H|$ divide n. Analogamente $|K|$ divide m. L'isomorfismo $G \cong H \times K$ permette di concludere $|H| \cdot |K| = mn$ e infine $|H| = n$ e $|K| = m$. □

Teorema 7.14. (Teorema di decomposizione primaria) *Sia G un gruppo abeliano finito di ordine n, $n \in \mathbb{N}_+$ e sia $n = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$, con p_i primo e $a_i \in \mathbb{N}_+$ per ogni $i = 1, \dots, t$, la decomposizione di n in prodotto di primi distinti. Allora esistono t sottogruppi $P_1, P_2, \dots, P_t$ di ordini rispettivamente $p_1^{a_1}, \dots, p_t^{a_t}$, tali che*

$$G \cong P_1 \times P_2 \times \dots \times P_t.$$

DIMOSTRAZIONE. La dimostrazione è per induzione su t. Se $t = 1$, il corollario è ovvio. Supponiamo $t \geq 2$ e sia $m = p_1^{a_1} \dots p_{t-1}^{a_{t-1}}$; allora m e $p_t^{a_t}$ sono coprimi e $mp_t^{a_t} = n$. Applichiamo la proposizione 7.13 per ottenere due sottogruppi H e P_t di ordini rispettivamente m e $p_t^{a_t}$ e tali che $G \cong H \times P_t$. Per l'ipotesi induttiva otteniamo $H \cong P_1 \times \dots \times P_{t-1}$ per certi sottogruppi $P_1, \dots, P_{t-1}$ di ordini rispettivamente $p_1^{a_1}, \dots, p_{t-1}^{a_{t-1}}$. Allora

$$G \cong H \times P_t \cong (P_1 \times \dots \times P_{t-1}) \times P_t \cong P_1 \times \dots \times P_{t-1} \times P_t,$$

che conclude la dimostrazione. □

Nel teorema 7.14 si dimostra quindi che se p è un primo che divide l'ordine di un gruppo abeliano finito G, allora esiste un p-sottogruppo di Sylow P. Inoltre dalla 7.13 si evince che $P = \{x \in G : o(x) = p^j \text{ per qualche } j \in \mathbb{N}\}$. Pertanto se H è un p-sottogruppo del gruppo G, H deve essere contenuto in P perché ogni suo elemento ha ordine una potenza del primo p. Questo prova anche che P è l'unico sottogruppo di Sylow di G.

Per concludere la dimostrazione del teorema di Frobenius-Stickelberger resta solo da dimostrare che i sottogruppi di Sylow P_i definiti nel teorema 7.14 si possono scrivere come prodotto di gruppi ciclici.

Teorema 7.15. *Siano p un numero primo, n un intero positivo e G un gruppo abeliano di ordine p^n. Allora G è isomorfo ad un prodotto diretto di gruppi ciclici.*

DIMOSTRAZIONE. Procediamo per induzione su n. Per $n = 1$ il gruppo stesso è ciclico, quindi non c'è niente da dimostrare. Se $n > 1$, scegliamo $b \in G$ con ordine massimo $p^k = o(b)$. Per il sottogruppo $B = \langle b \rangle$ scegliamo un sottogruppo $C \leq G$ tale che $B \cap C = \{0\}$ e C è massimale per questa proprietà, lo possiamo fare per il lemma 6.47. Dimostriamo che

$$G = B + C.$$

Sia $x \in G$; allora $o(x)$ divide $|G|$, pertanto $o(x) = p^s$ per qualche intero s con $0 \leq s \leq k$. Dimostriamo che $x \in B + C$ per induzione su s. Per $s = 0$, $x = 0 \in$

$B + C$. Supponiamo $s > 0$ e che tutti gli elementi di G di ordine p^{s-1} appartengano a $B + C$. Allora per $y = px$ si ha $o(y) = p^{s-1}$. Per l'ipotesi induttiva $y \in B + C$, cioè esistono $c \in C$ e $m \in \mathbb{Z}$ tali che

$$y = px = mb + c.$$

Moltiplicando per p^{s-1} troviamo $0 = p^{s-1}mb + p^{s-1}c$. Quindi

$$p^{s-1}mb \in C \cap B = \{0\}.$$

Allora $p^{s-1}mb = 0$ e per la scelta di b si ha che p^k divide $p^{s-1}m$. Di conseguenza p divide m e $m = pm_1$ con $m_1 \in \mathbb{Z}$, poiché $k > s - 1$. Allora $px = m_1pb + c$ e se poniamo $a = x - m_1b$, si ha $pa = c \in C$. Se $a \in C$, allora

$$x = a + m_1b \in B + C.$$

Se invece $a \notin C$, il sottogruppo $C_1 = \langle C, a\rangle$ contiene propriamente C, quindi $B \cap C_1 \neq \{0\}$ per la scelta di C. Sia $b' \in B \cap C_1$, $b' \neq 0$. Allora esistono $c \in C$ e $l \in \mathbb{Z}$ tali che $b' = c + la$. Se p divide l, allora esiste $l' \in \mathbb{Z}$ con $l = l'p$. Pertanto $la = l'pa \in C$, da cui $b' \in B \cap C = \{0\}$, in contraddizione con la scelta di $b' \neq 0$. Allora

$$(l,p) = 1, \quad la \in B + C \ \text{ e } \ pa \in C \leq B + C$$

implicano, per il lemma 7.10, $a \in B + C$. Ora anche

$$x = a + m_1b \in B + C.$$

Applichiamo il teorema 6.35 a

$$B, C \leq G, \quad G = B + C, \quad B \cap C = \{0\}$$

per ottenere

$$G \cong B \times C.$$

Poiché $|C| = |G|/|B| = p^{n-k}$, per l'ipotesi induttiva C è prodotto diretto di gruppi ciclici. Essendo B ciclico, anche G è prodotto diretto di gruppi ciclici. □

Possiamo ora dimostrare il teorema di Frobenius-Stickelberger.

Teorema 7.16. *Ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici.*

DIMOSTRAZIONE. Sia G un gruppo abeliano di ordine n. Sia $n = p_1^{a_1} \ldots p_t^{a_t}$ la scomposizione di n in prodotto di numeri primi distinti $p_1, \ldots, p_t$, con $a_i \in \mathbb{N}_+$ per $i = 1, \ldots, t$. Per il teorema 7.14 G è isomorfo al prodotto diretto $P_1 \times \ldots \times P_t$, dove $|P_i| = p_i^{a_i}$ per ogni $i = 1, \ldots, t$. Per il teorema 7.15 i sottogruppi P_i sono prodotti diretti di gruppi ciclici. Pertanto G è isomorfo a un prodotto diretto di gruppi ciclici. □

7.3 Alcuni gruppi abeliani infiniti

Esaminiamo alcune proprietà di uno dei gruppi infiniti più noti, cioè i numeri razionali. Altri risultati sui numeri razionali saranno presentati nell'esercizio 7.27.

Proposizione 7.17. *Ogni sottogruppo finitamente generato di* $(\mathbb{Q},+)$ *è ciclico.*

DIMOSTRAZIONE. Sia $H = \langle r_1, \ldots, r_n \rangle$, $n \in \mathbb{N}_+$ un sottogruppo finitamente generato di $\mathbb{Q}$. Sia $r_i = \frac{a_i}{b_i}$, con $a_i, b_i \in \mathbb{Z}$, $b_i \neq 0$. Allora, con $b = b_1 \ldots b_n$, H è un sottogruppo del gruppo ciclico $\langle 1/b \rangle$ ed è pertanto ciclico. □

Abbiamo dimostrato nel teorema 7.1 che $(\mathbb{Z},+)$ è l'unico gruppo ciclico infinito, a meno di isomorfismi. Inoltre ogni sottogruppo proprio di $\mathbb{Z}$ ha indice finito. Proviamo ora che questa proprietà caratterizza i gruppi ciclici infiniti.

Teorema 7.18. *Sia* $(G,+)$ *un gruppo abeliano infinito tale che ogni sottogruppo proprio di* G *ha indice finito. Allora* G *è ciclico.*

DIMOSTRAZIONE. Sia $x \in G$, $x \neq 0$. Allora $H = \langle x \rangle$ ha indice finito, quindi H è infinito. Questo dimostra che $o(x) = \infty$ per ogni $x \in G$, $x \neq 0$. Fissiamo un elemento non nullo $a \in G$ e sia $H_0 = \langle a \rangle$. Se $H_0 = G$ la dimostrazione è finita. Supponiamo che $H_0 \neq G$. Per $y \in G$, $y \neq 0$, il sottogruppo $\langle y \rangle$ ha indice finito, pertanto anche $\langle y \rangle \cap H_0$ ha indice finito per il lemma 5.61. In particolare

$$\langle y \rangle \cap H_0 \neq \{0\}.$$

Quindi esistono $n, m \in \mathbb{Z} \setminus \{0\}$ con $na = my$. Consideriamo l'applicazione $f : G \to \mathbb{Q}$ definita da

$$f(y) = \frac{n}{m} \quad \text{per} \quad y \in G, \;\; y \neq 0 \quad \text{e} \quad f(0) = 0.$$

Per vedere che la definizione è corretta, supponiamo di avere $m'y = n'a$ per un'altra coppia di interi $m', n' \in \mathbb{Z}$ e $m' \neq 0$. Allora moltiplicando per m si trova

$$mm'y = mn'a = nm'a \quad \text{perché} \quad na = my.$$

Ora $mn'a = nm'a$ implica $mn' = nm'$ perché a ha ordine infinito e

$$(mn' - nm')a = 0.$$

Concludiamo che $m/n = m'/n'$ e quindi f è definita correttamente. Inoltre f è un omomorfismo in quanto se $y, z \in G$ e uno dei due è 0, allora

$$f(y+z) = f(y) + f(z).$$

Se $y \neq 0 \neq z$, allora si ha

$$n_1 a = m_1 y \;\; \text{e} \;\; n_2 a = m_2 z \quad \text{per qualche } n_1, n_2, m_1, m_2 \in \mathbb{Z}^*.$$

Moltiplicando la prima uguaglianza per m_2 e la seconda per m_1, si ottiene

$$m_2 n_1 a = m_2 m_1 y \quad \text{e} \quad m_1 n_2 a = m_1 m_2 z$$

da cui $(m_2 n_1 + m_1 n_2)a = m_2 m_1 (y + z)$. Pertanto

$$f(y+z) = \frac{m_2 n_1 + m_1 n_2}{m_2 m_1} = \frac{n_1}{m_1} + \frac{n_2}{m_2} = f(y) + f(z).$$

Inoltre f ha nucleo $\{0\}$, quindi $G \cong f(G)$ e $f(G)$ ha la stessa proprietà. In particolare $\mathbb{Z} = f(H_0)$ ha indice finito in $f(G)$, quindi esistono un numero finito di classi laterali $q_1 + \mathbb{Z}, \ldots, q_r + \mathbb{Z}$ di $\mathbb{Z}$ in $f(G)$. Allora $f(G) = \langle 1, q_1, \ldots, q_r \rangle$ è finitamente generato. Per la proposizione 7.17 $f(G)$ è ciclico e quindi $G \cong f(G)$ è pure ciclico. □

Concludiamo il paragrafo sui gruppi abeliani infiniti introducendo i gruppi di Prüfer, che dimostreremo essere gli unici esempi di gruppi cociclici infiniti. Diamo la definizione di gruppo cociclico.

Per un gruppo G denotiamo con $\mathcal{U}_G$ l'unione di tutti sottogruppi propri di G. Allora si vede facilmente che G è ciclico se e solo se $\mathcal{U}_G$ non coincide con tutto G. In tal caso i possibili generatori di G sono precisamente gli elementi dell'insieme non vuoto $G \setminus \mathcal{U}_G$.

Questo punto di vista rende altrettanto importante la proprietà duale che nasce considerando l'*intersezione* $\mathcal{I}_G$ di tutti sottogruppi non nulli di un gruppo abeliano G.

Definizione 7.19. Il gruppo G si dice *cociclico* se il sottogruppo $\mathcal{I}_G$ è non nullo. In tal caso $\mathcal{I}_G$ è il più piccolo sottogruppo non nullo di G; ogni elemento non nullo di $\mathcal{I}_G$ sarà chiamato *cogeneratore* di G.

Chiaramente ogni cogeneratore è contenuto in ogni sottogruppo non nullo di G. Di conseguenza un omomorfismo $f : G \to H$ definito da un gruppo cociclico G ad un gruppo H è iniettivo se e solo se $f(c) \neq 0$ per qualche cogeneratore c di G, si veda l'esercizio 7.34.

È importante notare che alcuni gruppi non abeliani hanno la stessa proprietà dei gruppi cociclici abeliani, per esempio tutti i sottogruppi non banali di Q_8 contengono il centro $Z(Q_8)$ che non è banale. Perciò chiederemo esplicitamente che i gruppi in considerazione siano abeliani.

Esempio 7.20. Un gruppo ciclico finito $\mathbb{Z}_m$ è cociclico se e solo se m è della forma $m = p^k$ per qualche numero primo p e $k \in \mathbb{N}_+$. Infatti se $m = nl$ fosse prodotto di fattori coprimi, allora $\mathbb{Z}_m = \mathbb{Z}_n \times \mathbb{Z}_l$ per il teorema 6.42 e quindi avrebbe due sottogruppi non nulli con intersezione banale. D'altra parte, per il teorema 7.4 il gruppo $\mathbb{Z}_{p^k}$ ha un unico sottogruppo di ordine p che risulta contenuto in ogni sottogruppo non nullo di $\mathbb{Z}_{p^k}$, da cui $\mathbb{Z}_{p^k}$ è cociclico.

Questo esempio dimostra come i gruppi $\mathbb{Z}_{p^k}$ hanno la proprietà di essere simultaneamente ciclici e cociclici. Chiaramente il gruppo ciclico infinito $\mathbb{Z}$ non è cociclico. Vediamo un esempio di un gruppo cociclico infinito.

Esempio 7.21. Sia p un numero primo. Denotiamo con $\mathbb{Z}_{p^\infty}$ l'insieme di tutti gli elementi del gruppo quoziente $\mathbb{Q}/\mathbb{Z}$ del tipo $a/p^n + \mathbb{Z}$, con $a, n \in \mathbb{Z}$. Allora $\mathbb{Z}_{p^\infty}$ è un sottogruppo di $\mathbb{Q}/\mathbb{Z}$ e ponendo $c_n = 1/p^n + \mathbb{Z}$, per $n \in \mathbb{N}$, si vede facilmente che

$$o(c_n) = p^n \quad \text{e} \quad pc_n = c_{n-1} \quad \text{per} \quad n \in \mathbb{N}. \tag{1}$$

Pertanto il sottogruppo ciclico $C_n = \langle c_n \rangle$ di $\mathbb{Z}_{p^\infty}$ ha ordine p^n e

$$C_1 \leq C_2 \leq \ldots \leq C_n \leq \ldots . \tag{2}$$

Osserviamo che ogni $x \in \mathbb{Z}_{p^\infty}$ ha la forma $x = a/p^n + \mathbb{Z}$ e quindi $x = ac_n$, cioè

$$\mathbb{Z}_{p^\infty} = \bigcup_{n=1}^{\infty} C_n. \tag{3}$$

Ora da (2) e (3) deduciamo che

$$\mathbb{Z}(p^\infty) = C_1 \cup \bigcup_{n=1}^{\infty} (C_{n+1} \setminus C_n).$$

Poiché $C_{n+1} \setminus C_n$ è esattamente l'insieme di tutti i generatori di C_{n+1}, deduciamo che H contiene C_{n+1} se e solo se $H \cap (C_{n+1} \setminus C_n) \neq \emptyset$. Da (2) e (3) segue che un sottogruppo proprio H di $\mathbb{Z}(p^\infty)$ può contenere solo un numero finito dei sottogruppi C_n, quindi esiste $n \in \mathbb{N}$ tale che

$$H \cap (C_{m+1} \setminus C_m) = \emptyset$$

per tutti gli $m \geq n$. Di conseguenza $H \leq C_n$. Scegliamo il minimo n con questa proprietà, cioè H non è contenuto in C_{n-1}. Dunque $H = C_n$.

Definizione 7.22. Il gruppo $\mathbb{Z}_{p^\infty}$ dell'esempio 7.21 si dice *gruppo di Prüfer.*

Osserviamo che tutti i sottogruppi propri di $\mathbb{Z}_{p^\infty}$ sono finiti. Si può dimostrare che questa proprietà caratterizza $\mathbb{Z}_{p^\infty}$, si veda l'esercizio 7.37.

Dimostriamo infine che gli esempi 7.20 e 7.21 sono tutti e soli i gruppi cociclici, a meno di isomorfismo.

Teorema 7.23. *Sia C un gruppo abeliano cociclico. Allora esiste un numero primo p tale che $G \cong \mathbb{Z}_{p^\infty}$ oppure $G \cong \mathbb{Z}_{p^k}$ per qualche $k \in \mathbb{N}_+$.*

DIMOSTRAZIONE. Sia c_1 un cogeneratore di G. Allora il sottogruppo ciclico

$$C_1 = \langle c_1 \rangle$$

non ha sottogruppi propri, pertanto $C_1 \cong \mathbb{Z}_p$ per qualche numero primo p. Inoltre, se $x \neq 0$, il sottogruppo ciclico $\langle x \rangle$ contiene C_1. Quindi $o(x)$ è una potenza di p. Dimostriamo per induzione su n che se $p^n \leq |G|$, allora il gruppo G ha esattamente un sottogruppo di ordine p^n e tale sottogruppo è ciclico. Per $n = 1$ l'asserto è vero.

Sia $n \geq 1$, tale che $p^n \leq |G|$. Supponiamo che G abbia un solo sottogruppo C_n di ordine p^n e $C_n = \langle c_n \rangle$. Se $G = C_n$ la dimostrazione è finita. Altrimenti esiste $x \in G \setminus C_n$ tale che $o(x) = p^k$ per qualche $k \in \mathbb{N}_+$. L'ipotesi su C_n implica $k > n$. Pertanto esistono elementi di periodo p^{n+1} in G e quindi anche sottogruppi di G di ordine p^{n+1}. Siano A e B sottogruppi di G con $|A| = |B| = p^{n+1}$. Dimostreremo che $B \leq A$ e quindi $A = B$. Siano $a \in A \setminus C_n$ e $b \in B \setminus C_n$. Allora

$$o(a) = o(b) = p^{n+1} \text{ e quindi } \; pa, pb \in C_n.$$

Sia $pa = mc_n$, con $m \in \mathbb{Z}$. Dal fatto che $o(pa) = p^n$, si ha $(m, p) = 1$, in particolare pa è un generatore di C_n. Quindi esiste $k \in \mathbb{N}_+$ tale che $pb = kpa$. Se $b = ka$, abbiamo già $b \in A$ come desiderato. Altrimenti l'elemento $t = b - ka$ di G è non nullo e soddisfa $pt = 0$. Per il caso $n = 1$ possiamo concludere che $t \in C_1$. Pertanto $b \in A + C_1$. Poiché si ha $C_1 \leq C_n \leq A$, si conclude che $b \in A$.

Se il gruppo G è finito, avremo ad un certo passo $G = C_n$. Altrimenti

$$G = \bigcup_{n=1} C_n,$$

dove i sottogruppi ciclici C_n di G soddisfano (2). Concludiamo facilmente che $G \cong \mathbb{Z}_{p^\infty}$. □

7.4 Esercizi sui gruppi abeliani

Esercizio 7.1 Descrivere tutti i gruppi abeliani di ordine minore o uguale a 15 senza far ricorso al teorema 7.16.

Esercizio 7.2 Sia G un gruppo abeliano di ordine n, dove n =6, 12, 18, 22, 24, 28, 30, 33, 35, 42, 46, 66, 69, 78, 102, 105, 106, 110, 114, 119, 130, 131. Si dica per quali n si può affermare che G è necessariamente ciclico.

Esercizio 7.3 Determinare il numero dei gruppi abeliani di ordine 24 a meno di isomorfismo. Lo stesso per quelli di ordine 100 e 144. Sia p un numero primo; quanti sono a meno di isomorfismo i gruppi abeliani di ordine p^5?

Esercizio 7.4 Siano p, q ed r numeri primi distinti. Quanti sono i gruppi abeliani di ordine $p^5q^4r^3$ a meno di isomorfismo?

Esercizio 7.5 Sia G un gruppo abeliano di ordine pq, con p e q primi non necessariamente distinti. Calcolare tutti i sottogruppi di G.

Esercizio 7.6 Siano m un numero intero positivo e G un gruppo. È vero che il sottoinsieme $H = \{x \in G : x^n = 1\}$ di G è un sottogruppo di G?

Esercizio 7.7 Sia G un gruppo abeliano finito. Sia G^* l'insieme di tutti gli omomorfismi $f : G \to \mathbb{R}/\mathbb{Z}$ sul quale definiamo un'operazione

$$(f + g)(x) = f(x) + g(x).$$

Si dimostri che G^* è un gruppo e che se $G = H \times K$, allora $G^* \cong H^* \times K^*$.

Esercizio 7.8 * Sia G un gruppo abeliano finito e G^* il gruppo degli omomorfismi $f : G \to \mathbb{R}/\mathbb{Z}$ definito nell'esercizio 7.7. Si dimostri che se G è ciclico, allora $G \cong G^*$.

Esercizio 7.9 Sia G un gruppo abeliano finito e G^* il gruppo degli omomorfismi $f : G \to \mathbb{R}/\mathbb{Z}$ definito nell'esercizio 7.7. Si dimostri che $G \cong G^*$.

Esercizio 7.10 Siano p un numero primo e $G = \langle x, y \rangle$ un gruppo abeliano finito tale che p divide $|G|$, ma p non divide $o(x)$. Dimostrare che p divide $o(y)$.

Esercizio 7.11 Se p è un numero primo e $G = \mathbb{Z}_{p^k}^m$, $m \in \mathbb{N}_+, k \in \mathbb{N}$ calcolare il numero degli elementi $x \in G$ con $o(x) = p^s$, $s \in \mathbb{N}$.

Esercizio 7.12 Se p è un numero primo, $r, s, m_s \in \mathbb{N}$ e $G = \mathbb{Z}_p^{m_1} \times \mathbb{Z}_{p^2}^{m_2} \times \ldots \times \mathbb{Z}_{p^s}^{m_s}$ con $m_s > 0$, calcolare il numero degli elementi $x \in G$ con $o(x) = p^r$.

Esercizio 7.13 * Siano G ed H gruppi abeliani finiti. Se per ogni $k \in \mathbb{N}$ c'è un numero uguale di elementi di periodo k in G ed H, dimostrare che G ed H sono isomorfi.

Esercizio 7.14 Sia A un gruppo non identico e sia $\tau : A \to A$ l'applicazione definita da $\tau(a) = a^{-1}$. Si dimostri che:

(a) τ è biettiva;

(b) l'applicazione τ è un omomorfismo (quindi un automorfismo) di gruppi se e solo se A è abeliano;

(c) se ogni elemento non identico di A ha ordine 2, allora τ è l'identità, altrimenti τ ha ordine 2 quale elemento del gruppo $\mathrm{Aut}(A)$.

Esercizio 7.15 Sia $f \in \mathrm{Aut}(\mathbb{Q}, +)$. Dimostrare che:

(a) esiste $r \in \mathbb{Q}, r \neq 0$, tale che $f(x) = rx$ per ogni $x \in \mathbb{Q}$;
(b) $\mathrm{Aut}(\mathbb{Q}, +) \cong (\mathbb{Q}^*, \cdot)$;
(c) $\mathrm{Aut}(\mathbb{Q} \times \mathbb{Q}, +) \cong GL_2(\mathbb{Q})$;
(d) $\mathrm{Aut}(\mathbb{Q}^n, +) \cong GL_n(\mathbb{Q})$.

Esercizio 7.16 Descrivere $\mathrm{Aut}(\mathbb{Z}_n)$, con $n = 3, 5, 7, 8, 9, 11, 13, 20, 21, 22, 24, 29, 33, 44, 35, 36, 59, 60, 68, 72, 210$.

Esercizio 7.17 Sia $n \geq 3$ un intero. Dimostrare che il numero $|\mathrm{Aut}(\mathbb{Z}_n)|$ è pari.

Esercizio 7.18 Sia $f : G \to H$ un omomorfismo di gruppi tali che $|G| = m$ e $|H| = n$, con $m, n \in \mathbb{N}_+$, $(m, n) = 1$. Allora f è banale, cioè $\ker f = G$.

Esercizio 7.19 Siano m ed n interi positivi coprimi. Allora ogni omomorfismo

$$f : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$$

ha la forma $f = (f_1, f_2)$, dove $f_1 : \mathbb{Z}_m \to \mathbb{Z}_m$ e $f_2 : \mathbb{Z}_n \to \mathbb{Z}_n$ sóno opportuni omomorfismi (si veda l'esercizio 6.17).

Esercizio 7.20 Sia $G = \mathbb{Z}_m \times \mathbb{Z}_n$, con $n, m \in \mathbb{N}_*$, $(m, n) = 1$. Dimostrare che

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathbb{Z}_m) \times \mathrm{Aut}(\mathbb{Z}_n).$$

Esercizio 7.21 Siano m e n interi positivi coprimi e siano G ed H gruppi abeliani con $|G| = m$ e $|H| = n$. Allora ogni automorfismo $f : G \times H \to G \times H$ ha la forma $f = (f_1, f_2)$, dove $f_1 \in \mathrm{Aut}(G)$ e $f_2 \in \mathrm{Aut}(H)$.

Esercizio 7.22 Sia p un numero primo. Dimostrare che $\mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p) \cong GL_2(\mathbb{F}_p)$.

Esercizio 7.23 * Provare che ogni gruppo G di ordine 15 è ciclico.

Esercizio 7.24 Siano p e q numeri primi distinti. Provare che ogni gruppo abeliano di ordine pq è ciclico.

Esercizio 7.25 * Descrivere $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4)$.

Esercizio 7.26 Sia $G = \mathbb{Z} \times \mathbb{Z}$ il prodotto diretto di due copie di $\mathbb{Z}$.

(a) Si provi che tutti gli elementi di G sono aperiodici.
(b) Si dimostri che l'applicazione $f : G \to G$ tale che $f(i, j) = (-i, j)$ per ogni $i, j \in \mathbb{Z}$ è un automorfismo di G; si determini il periodo di f come elemento di $\mathrm{Aut}(G)$.
(c) Se π_1 è la proiezione di G sulla prima componente $\mathbb{Z}$, si definisca un automorfismo φ di G tale che $(\pi_1 \circ \varphi)(i, j) = i + j$ per ogni $i, j \in \mathbb{Z}$.
(d) È vero che $\mathrm{Aut}(G)$ contiene un sottogruppo non ciclico di ordine 4?
(e) Dimostrare che $\mathrm{Aut}(G)$ è isomorfo al sottogruppo di $GL_2(\mathbb{Z})$ formato dalle matrici con coefficienti interi.

Esercizio 7.27 Dimostrare che ogni sottogruppo finitamente generato di $\mathbb{Q}/\mathbb{Z}$ è ciclico.

Esercizio 7.28 * Dimostrare che il gruppo abeliano $\mathbb{Q} \times \mathbb{Q}$ non è isomorfo a $\mathbb{Q}$. Dimostrare che il gruppo abeliano $\mathbb{R} \times \mathbb{R}$ è isomorfo a $\mathbb{R}$.

Esercizio 7.29 Provare che i gruppi $(\mathbb{Z}_8, +)$ e $Aut(\mathbb{Z}_{15})$ non sono isomorfi.

Esercizio 7.30 Sia G un gruppo abeliano di ordine $m > 1$. Provare che il gruppo G non è ciclico se e solo se esiste un divisore proprio n di m tale che $nx = 0$ per ogni $x \in G$. Pertanto G è ciclico se e solo se $\exp(G) = |G|$.

Esercizio 7.31 * Siano $s, k_1, \ldots, k_s \in \mathbb{N}_+$ e $m = p_1^{k_1} \ldots p_s^{k_s}$, con $p_1, \ldots, p_s$ numeri primi dispari distinti. Provare che

$$\mathrm{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_{p_1^{k_1} - p_1^{k_1 - 1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s} - p_s^{k_s - 1}}.$$

Esercizio 7.32 Descrivere i sottogruppi di:

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2$;
(b) $\mathbb{Z}_2 \times \mathbb{Z}_3$;

(c) $\mathbb{Z}_3 \times \mathbb{Z}_3$;
(d) $\mathbb{Z}_2 \times \mathbb{Z}_4$;
(e) $\mathbb{Z}_8 \times \mathbb{Z}_9$;
(f) $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
(g) $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

Esercizio 7.33 Dimostrare che il sottogruppo

$$V = \{id, (12)(34), (13)(24), (14)(23)\}$$

del gruppo simmetrico S_4 è isomorfo al gruppo $\mathrm{Aut}(\mathbb{Z}_8)$.

Esercizio 7.34 Sia G un gruppo abeliano cociclico e sia c un cogeneratore di G. Dimostrare che un omomorfismo $f : G \to H$ è iniettivo se e solo se $c \notin \ker f$.

Esercizio 7.35 Un sottogruppo proprio M di un gruppo G si dice *massimale*, se ogni sottogruppo proprio di G contenente M coincide con M. Dimostrare che:

(a) ogni gruppo finito possiede sottogruppi massimali;
(b) un gruppo ciclico finito $\mathbb{Z}_m$, $m \in \mathbb{N}_+$, possiede un solo sottogruppo massimale se e solo se $m = p^k$ per un primo p e un numero naturale non nullo k;
(c) i sottogruppi massimali di $\mathbb{Z}$ sono $p\mathbb{Z}$, dove p è un numero primo;
(d) * i gruppi $(\mathbb{Q}, +)$ e $(\mathbb{Z}_{p^\infty}, +)$, per ogni numero primo p, non hanno sottogruppi massimali;
(e) se p è un primo e se tutti gli elementi non nulli di un gruppo abeliano G hanno periodo p, allora ogni sottogruppo proprio di G è contenuto in qualche sottogruppo massimale;
(f) se $f : G \to G_1$ è un omomorfismo suriettivo e M è un sottogruppo massimale di G_1, allora $f^{-1}(M)$ è un sottogruppo massimale di G.

Esercizio 7.36 Dimostrare che per un gruppo abeliano G sono equivalenti le seguenti condizioni:

(a) G ha sottogruppi massimali;
(b) esiste un numero primo p tale che il sottogruppo $pG = \{px : x \in G\}$ di G è proprio;
(c) esistono un numero primo p e un elemento $x \in G$ tali che x non si può scrivere come $x = py$ per alcun elemento $y \in G$.

Dare una nuova dimostrazione al fatto che $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{Z}_{p^\infty}$, per ogni numero primo p, non hanno sottogruppi massimali.

Esercizio 7.37 * Sia G un gruppo abeliano infinito tale che ogni sottogruppo proprio di G sia finito. Dimostrare che $G \cong \mathbb{Z}_{p^\infty}$ per qualche primo p.

8

I gruppi non abeliani: un primo approccio

In questo capitolo ci proponiamo di introdurre lo studio dei gruppi non abeliani. Rivolgeremo il nostro studio quasi prevalentemente ai gruppi non abeliani finiti.

Tutti i gruppi di ordine un primo p sono abeliani e così i gruppi di ordine 4. Quindi per trovare un gruppo non abeliano dobbiamo supporre $|G|$ maggiore o uguale a 6. Proviamo nell'esercizio 8.1 che S_3 è l'unico gruppo non abeliano di ordine 6.

Si può dimostrare che ci sono solo due gruppi non abeliani di ordine 8, a meno di isomorfismo: il gruppo dei quaternioni Q_8 e il gruppo diedrale D_8 introdotto nell'esercizio 5.51. Proveremo nella proposizione 8.16 che i gruppi di ordine p^2 sono abeliani, per ogni primo p e che quelli di ordine 15 sono ciclici. Si può dimostrare che gli unici gruppi non abeliani di ordine 10 e 14 sono esattamente quelli descritti negli esercizi 5.52 e 5.54. Infine ci sono tre gruppi non abeliani di ordine 12, a meno di isomorfismo: il gruppo alterno A_4, il prodotto diretto $S_3 \times \mathbb{Z}_2$ ed un gruppo G tale che G ha esponente 12, il centro di G ha ordine 2 e $G/Z(G)$ è isomorfo a S_3.

Queste osservazioni permettono di classificare tutti i gruppi di ordine minore o uguale 15. La situazione diventa decisamente più complessa se si considerano i gruppi di ordine 16: oltre ai cinque abeliani, ve ne sono altri nove non abeliani.

Nel primo paragrafo si introducono alcuni sottogruppi normali per un qualsiasi gruppo (non abeliano). Nel secondo paragrafo si prova un'utile equazione sull'ordine delle classi di coniugio nei gruppi finiti. Dimostriamo in seguito il lemma di Cauchy e il teorema di Sylow, che garantiscono l'esistenza di sottogruppi di un certo ordine fissato in un gruppo finito. Nel terzo paragrafo proviamo che il gruppo alterno A_n è un gruppo semplice per $n > 4$. Il quarto paragrafo introduce un concetto importantissimo, quello di *azione* di gruppo su un insieme. Questo è il modo concreto in cui talvolta viene introdotto il concetto di gruppo, anziché nel modo astratto da noi adottato nella definizione 4.11. Si dimostrano infine il secondo e il terzo teorema di Sylow.

8.1 Alcuni sottogruppi normali

Una conseguenza del fatto che il gruppo non è abeliano è che non tutti i sottogruppi sono necessariamente normali. Iniziamo quindi lo studio dei gruppi non abeliani, cercando innanzitutto di capire quali sottogruppi sono normali. Abbiamo già visto nel lemma 5.72 che il centro di un gruppo è un sottogruppo normale. Introduciamo ora un altro sottogruppo normale di G.

Definizione 8.1. Dati due elementi a, b di un gruppo G, si denota con $[a, b]$ l'elemento $a^{-1}b^{-1}ab$, che si chiama *commutatore di a e b* .

Si osservi che $ab = ba(ba)^{-1}ab = ba(a^{-1}b^{-1}ab) = ba[a, b]$, da cui segue immediatamente $[a, b] = 1$ se e solo se a, b commutano, come visto nel lemma 5.1.

Osservazione 8.2. Sia N un sottogruppo normale di un gruppo G. Allora $[n, g] \in N$ per ogni $n \in N$, $g \in G$. Infatti $[n, g] = n^{-1}g^{-1}ng = n^{-1}n^g \in N$, perché $n^g \in N$.

Consideriamo ora il sottogruppo generato da tutti i commutatori di un gruppo. Anche questo sottogruppo risulta essere normale, anzi risulta essere caratteristico.

Definizione 8.3. Siano G un gruppo ed H un sottogruppo di G. Allora H si dice *caratteristico in* G se $H^\varphi \leq H$ per ogni automorfismo φ di G.

Se H è un sottogruppo caratteristico di un gruppo G, allora H è normale in G. Infatti per ogni $g \in G$, il coniugio φ_g tramite g è un automorfismo di G e quindi

$$H^g = H^{\varphi_g} \leq H.$$

Nell'esercizio 8.7 si prova che se $H \leq K \leq G$, H è caratteristico in K, K è caratteristico in G, allora H è caratteristico in G.

Lemma 8.4. *Sia* $G' = \langle [a, b] : a, b \in G \rangle$ *il sottogruppo generato dai commutatori di G. Allora* G' *è un sottogruppo caratteristico di G.*

DIMOSTRAZIONE. È sufficiente verificare che se x è un generatore di G' e $\varphi \in \mathrm{Aut}(G)$, allora $x^\varphi \in G'$. Sia $x = [a, b]$ e $\varphi \in \mathrm{Aut}(G)$, allora:

$$x^\varphi = [a, b]^\varphi = (a^{-1}b^{-1}ab)^\varphi = (a^\varphi)^{-1}(b^\varphi)^{-1}a^\varphi b^\varphi = [a^\varphi, b^\varphi] \in G'.$$

Poiché vale per i generatori di G', vale anche per elementi arbitrari di G'. □

Il sottogruppo caratteristico G' di G definito nel lemma 8.4 si chiama *sottogruppo derivato di* G, o più semplicemente il *derivato* di G. Verifichiamo che il quoziente G/G' è abeliano e anzi dimostriamo che G' è il più piccolo sottogruppo con questa proprietà.

Lemma 8.5. *Sia* G' *il sottogruppo derivato di un gruppo G e* $N \trianglelefteq G$*. Allora* G/N *è abeliano se e solo se* $N \geq G'$.

DIMOSTRAZIONE. Osserviamo che G/N è abeliano se e solo se per ogni $a, b \in G$, si ha $aNbN = abN = baN = bNaN$ se e solo se $a^{-1}b^{-1}ab \in N$ se e solo se $G' \leq N$. □

Da questo corollario segue facilmente che ogni sottogruppo di G contenente G' è normale.

Siano G un gruppo ed H un suo sottogruppo; introduciamo due sottogruppi normali in G legati ad H.

Definizione 8.6. Si dice *cuore* di H in G e si denota con H_G il sottogruppo generato dai sottogruppi normali di G contenuti in H. Si dice *chiusura normale* di H in G e si denota H^G l'intersezione dei sottogruppi normali che contengono H.

Osserviamo che grazie al lemma 5.69 H_G risulta essere il più grande sottogruppo normale di G contenuto in H e H^G il più piccolo sottogruppo normale di G contenente H.

Possiamo caratterizzare questi due sottogruppi nel modo seguente.

Proposizione 8.7. *Siano G un gruppo e H sottogruppo di G. Allora*

$$H_G = \bigcap_{x \in G} H^x \quad e \quad H^G = \langle H^x : x \in G \rangle.$$

DIMOSTRAZIONE. Per il lemma 5.69 H_G è normale e pertanto per ogni $x \in G$ si ha $H_G = H_G^x \leq H^x$ da cui segue che $H_G \leq \bigcap_{x \in G} H^x$. Viceversa siano $g \in G$ e $u \in \bigcap_{x \in G} H^x$. Fissiamo ora un elemento $x \in G$ arbitrario. Dal fatto che $u \in (xg^{-1})^{-1}H(xg^{-1}) = gx^{-1}Hxg^{-1}$ segue che esiste $h \in H$ tale che $u = gx^{-1}hxg^{-1}$ e quindi $g^{-1}ug = x^{-1}hx \in H^x$. Essendo x arbitrario concludiamo che

$$g^{-1}ug \in \bigcap_{x \in G} H^x.$$

Di conseguenza $\bigcap_{x \in G} H^x$ è un sottogruppo normale contenuto in H e dunque è contenuto in H_G.

Sia ora $x \in G$; allora $H^x \leq (H^G)^x \leq H^G$ perché H^G è normale per il lemma 5.69. Pertanto $\langle H^x : x \in G \rangle \leq H^G$. Vediamo viceversa che $\langle H^x : x \in G \rangle$ è un sottogruppo normale che contiene H, da cui seguirà che $H^G \leq \langle H^x : x \in G \rangle$. Per $a \in \langle H^x : x \in G \rangle$, si ha $a = a_1 \dots a_n$, con $a_i \in H^{x_i}$ per $i = 1, \dots, n$, $n \in N_+$. Se $g \in G$, allora $a_i^g \in (H^{x_i})^g = g^{-1}x_i^{-1}Hx_ig = (x_ig)^{-1}H(x_ig)$. Pertanto

$$a^g = g^{-1}ag = (g^{-1}a_1g)(g^{-1}a_2g)\dots(g^{-1}a_ng) \in \langle H^x : x \in G \rangle.$$

Quindi per il lemma 5.67 $\langle H^x : x \in G \rangle$ è normale e contiene H e dunque contiene H^G. □

Chiaramente H_G è contenuto in H e risulta $H_G = H$ se e solo se il sottogruppo H è normale. Nell'esercizio 8.6 chiediamo di provare che H_G contiene l'intersezione $H \cap Z(G)$ e ciò fornisce un limite *inferiore* per il cuore H_G.

Daremo alcuni esempi in cui l'uguaglianza $H \cap Z(G) = H_G$ vale. Affinché ciò accada è sufficiente che sia verificata l'inclusione $\bigcap_{x \in G} H^x \leq Z(G)$. Nei casi concreti bastano addirittura anche intersezioni di due o tre coniugati di H, come ad esempio nell'esercizio 8.25.

8.2 Centralizzanti, equazione delle classi e lemma di Cauchy

Abbiamo visto la definizione di elemento centrale. Può accadere però che in un gruppo non ci siano elementi centrali non banali, come ad esempio nei gruppi simmetrici S_n, con $n \geq 3$, si veda l'esercizio 8.3. Diamo la definizione di centralizzante di un sottoinsieme X di un gruppo G.

Definizione 8.8. Un elemento g di G *centralizza* X se $gx = xg$ per ogni $x \in X$.
L'insieme $C_G(X) = \{g \in G : gx = xg \ \forall x \in X\}$ degli elementi di G che centralizzano X si chiama *centralizzante di* X *in* G.

Per non appesantire la notazione scriveremo $C_G(x)$ per indicare il centralizzante dell'insieme $\{x\}$. Calcoliamo il centralizzante di alcuni elementi.

Esempio 8.9. Consideriamo l'elemento (12) di $G = S_3$. Allora

$$C_{S_3}((12)) = \langle (12) \rangle.$$

Se invece consideriamo (12) come elemento di S_4, avremo

$$C_{S_4}((12)) = \langle (12), (34) \rangle.$$

Dato un gruppo G, possiamo definire la relazione

$$x \sim_G y \quad \text{se e solo se esiste} \quad g \in G \quad \text{tale che} \quad y = x^g.$$

Si dimostra facilmente che $\sim_G$ è una relazione di equivalenza, si veda l'esercizio 5.57. Possiamo allora considerare le classi di equivalenza rispetto a $\sim_G$.

Definizione 8.10. Siano G un gruppo e x un elemento di G. La *classe di coniugio* di x è la classe di equivalenza di x rispetto a $\sim_G$, cioè l'insieme dei coniugati di x in G. Si denota con $x^G = \{x^g : g \in G\}$.

Si ha $1^G = \{1\}$ e più in generale la classe di coniugio di un elemento x di un gruppo G coincide con il singoletto $\{x\}$ precisamente quando x è un elemento centrale. Infatti $x^G = \{x\}$ se e solo se $x^g = x$ per ogni $g \in G$, cioè x commuta con tutti gli elementi di G.

Supponiamo ora che G sia un gruppo finito. Siano $x_1, \ldots, x_t$ i rappresentanti delle classi di coniugio di G di elementi non centrali, cioè $|x_i^G| > 1$ per ogni $i = 1, \ldots, t$. Le classi di equivalenza costituiscono una partizione e, se si raggruppano tutte le classi di equivalenza che contengono un solo elemento, allora

$$\{x \in G : |x^G| = 1\} = Z(G).$$

Otteniamo quindi la partizione

$$G = Z(G) \cup x_1^G \cup x_2^G \cup \ldots \cup x_t^G.$$

Calcolando la cardinalità di questi insiemi disgiunti segue l'*equazione delle classi*:

$$|G| = |Z(G)| + \sum_{i=1}^{t} |x_i^G|. \tag{1}$$

La prossima proposizione mette in relazione il numero dei coniugati di un elemento con il suo centralizzante.

Proposizione 8.11. *Siano G un gruppo e X un sottoinsieme di G. Allora:*

(a) $C_G(X)$ è un sottogruppo di G che contiene il centro di G;
(b) per ogni sottogruppo H di G si ha $C_G(H) \cap H = Z(H)$; in particolare $C_G(G) = Z(G)$;
(c) $|x^G| = [G : C_G(x)]$.

DIMOSTRAZIONE. (a) Siano $g_1, g_2 \in C_G(X)$ e sia $x \in X$. Allora $g_1 x = x g_1$ e $g_2 x = x g_2$ implicano

$$x g_1^{-1} = g_1^{-1} x \quad \text{e} \quad (g_1 g_2) x = g_1 (g_2 x) = (g_1 x) g_2 = x (g_1 g_2).$$

Quindi $C_G(X)$ è un sottogruppo e contiene il centro di G perché ogni elemento del centro commuta in particolare con gli elementi di X.

(b) Si ha $C_G(H) \cap H = \{g \in H : gh = hg \ \forall h \in H\} = Z(H)$.

(c) Sia x^G la classe di coniugio di x in G. Siano $C = C_G(x)$ e $\mathcal{C}$ l'insieme delle classi laterali destre del sottogruppo C in G. Definiamo $f : \mathcal{C} \to x^G$ con $f(Cg) = x^g$. Dimostriamo che f è ben definita e iniettiva:

$$Cg = Ch \iff gh^{-1} \in C \iff (gh^{-1})x = x(gh^{-1}) \iff$$

$$g^{-1} x g = h^{-1} x h \iff f(Cg) = f(Ch).$$

Dalla definizione di x^G segue che f è suriettiva. Pertanto f è una biezione e quindi gli insiemi $\mathcal{C}$ e x^G hanno la stessa cardinalità. Si conclude osservando che

$$|\mathcal{C}| = [G : C_G(x)].$$

□

Abbiamo dimostrato il lemma 7.11 di Cauchy nel caso dei gruppi abeliani finiti. Siamo ora in grado di provarlo per un qualsiasi gruppo finito G.

Lemma 8.12. (Lemma di Cauchy) *Sia p un primo che divide l'ordine di G. Allora esiste in G un elemento di ordine p.*

DIMOSTRAZIONE. Sia $|G| = pm$, $m \in \mathbb{N}_+$; dimostriamo il lemma per induzione su m. Per $m = 1$ il lemma è ovvio, anzi ogni elemento non identico di G ha ordine proprio p.

Supponiamo $m > 1$. Se esiste $H < G$ tale che p divide $|H|$, per induzione esiste un elemento x in H tale che $o(x) = p$ e tale x appartiene anche a G. Supponiamo per

assurdo che p non divida l'ordine di alcun sottogruppo proprio di G. Per il lemma di Cauchy 7.11 dimostrato nel caso abeliano, G non è abeliano e quindi $Z(G) \neq G$. Sia $a \notin Z(G)$, allora $C_G(a) < G$ e poiché p non divide $|C_G(a)|$, per il teorema di Lagrange 5.52 p divide $[G : C_G(a)]$ e quindi p divide $|a^G|$ da (c) della proposizione 8.11. Poiché questo è vero per ogni elemento non centrale, dall'equazione delle classi ricaviamo che $|G| \equiv_p |Z(G)|$ e poiché $|G| \equiv_p 0$ e $|Z(G)| \geq 1$, si conclude che p divide $|Z(G)|$, assurdo poiché $Z(G)$ è un sottogruppo proprio di G e quindi per la nostra ipotesi p non divide $|Z(G)|$. □

Grazie al lemma di Cauchy 8.12 possiamo ora caratterizzare l'ordine di un p-gruppo finito, con p primo.

Lemma 8.13. *Siano G un gruppo finito e p un primo. Allora G è p-gruppo se e solo se $|G| = p^m$ per qualche m in $\mathbb{N}$.*

DIMOSTRAZIONE. Se $|G| = p^m$, allora per il corollario 5.54 ogni elemento di G ha ordine una potenza di p.

Sia G gruppo tale che ogni elemento di G abbia ordine una potenza di p. Supponiamo per assurdo che esista un primo $q \neq p$ tale che q divide l'ordine di G. Allora per il lemma di Cauchy 8.12 esiste un elemento di ordine q, contraddicendo l'ipotesi. □

Un'altra importante conseguenza dell'equazione delle classi, nel caso dei p-gruppi, è la seguente.

Lemma 8.14. *Siano p un primo e G un p-gruppo finito. Allora il centro di G non è banale.*

DIMOSTRAZIONE. Consideriamo l'equazione delle classi applicata a G. Siano x_1, ..., x_t, per $t \in \mathbb{N}$ i rappresentanti delle classi di coniugio di G di elementi non centrali, cioè per ogni $i = 1, \ldots, t$ si ha

$$|x_i^G| > 1 \quad \text{e} \quad G = Z(G) \cup x_1^G \cup x_2^G \cup \ldots \cup x_t^G.$$

Allora per il lemma 8.11 $|x_i^G| = [G : C_G(x_i)] > 1$ e per il teorema di Lagrange 5.52 $[G : C_G(x_i)]$ divide l'ordine di G per $i = 1, 2, \ldots, t$. Per il lemma 8.13 si ha

$$|x_i^G| = [G : C_G(x_i)] \equiv_p 0$$

per ogni $i = 1, 2, \ldots, t$. Da ciò segue che

$$0 \equiv_p |G| = |Z(G)| + |x_1^G| + |x_2^G| + \ldots + |x_t^G| \equiv_p |Z(G)|.$$

Quindi p divide $|Z(G)|$ e poiché $Z(G)$ non è vuoto perché contiene almeno l'elemento identico, segue che $|Z(G)| \geq p$. □

Una conseguenza del lemma 8.14 appena visto e del seguente lemma 8.15 è il fatto che tutti i gruppi di ordine p^2, con p primo, sono abeliani.

Lemma 8.15. *Sia G un gruppo e $Z(G)$ il centro di G. Se $G/Z(G)$ è ciclico, allora G è abeliano.*

DIMOSTRAZIONE. Supponiamo per assurdo che G non sia abeliano; allora

$$|G/Z(G)| > 1.$$

Poiché $G/Z(G)$ è ciclico, esiste $g \in G$ tale che $G/Z(G) = \langle \overline{g} \rangle$, con $\overline{g} = gZ(G)$. Allora per ogni $x, y \in G$, si ha che $xZ(G) = \overline{g}^i$ e $yZ(G) = \overline{g}^j$, per qualche $i, j \in \mathbb{N}$. Da questo si ricava che $x = z_1 g^i$ e $y = z_2 g^j$ con $z_1, z_2 \in Z(G)$ e quindi

$$xy = z_1 g^i z_2 g^j = z_1 z_2 g^i g^j = z_2 z_1 g^j g^i = z_2 g^j z_1 g^i = yx,$$

che contraddice l'ipotesi che G non sia abeliano. □

Proposizione 8.16. *Siano p un primo e G un gruppo di ordine p^2. Allora G è abeliano.*

DIMOSTRAZIONE. Poiché G è un p-gruppo, si ha $\{1\} \neq Z(G)$ per il lemma 8.14. Per il teorema di Lagrange 5.52 $|Z(G)| = p$ o p^2. Se $Z(G) = p^2$, $Z(G) = G$ e G è abeliano. Se fosse $|Z(G)| = p$, allora $G/Z(G)$ avrebbe ordine p e pertanto sarebbe un gruppo ciclico di ordine p. Per il lemma 8.15 questo non può accadere. □

A questo punto viene spontaneo chiedersi che cosa accade se si considerano gruppi di ordine p^3. Il gruppo dei quaternioni Q_8 e il gruppo diedrale D_8 sono esempi di gruppi non abeliani di ordine 8. Inoltre i gruppi definiti nell'esercizio 6.2 (d) sono gruppi non abeliani di ordine p^3.

Possiamo dimostrare ora il primo teorema di Sylow.

Teorema 8.17. (Primo teorema di Sylow) *Sia G gruppo finito, tale che $|G| = n = p^a m$, con p primo, $a \in \mathbb{N}_+$ e $(p, m) = 1$. Allora G ha un p-sottogruppo di Sylow di ordine p^a.*

DIMOSTRAZIONE. Lo dimostriamo per induzione su $n = |G|$. Se $n = 1$ non c'è nulla da dimostrare. Sia $n > 1$ e supponiamo il teorema vero per ogni gruppo di ordine strettamente minore di n. Consideriamo l'equazione delle classi per G

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)],$$

ove gli elementi x_i sono i rappresentanti delle classi di coniugio non centrali di G. Se esiste $i \in \{1, \dots, t\}$ tale che p non divide $[G : C_G(x_i)]$, allora poiché p^a divide $|G|$ e per il teorema di Lagrange 5.52,

$$|G| = [G : C_G(x_i)] |C_G(x_i)|;$$

concludiamo che p^a divide $|C_G(x_i)|$. L'elemento x_i non appartiene al centro di G e pertanto $C_G(x_i) < G$. Applicando l'ipotesi induttiva a $C_G(x_i)$, otteniamo un sottogruppo P di ordine p^a, che è pertanto un p-sottogruppo di Sylow anche di G.

Possiamo supporre che p divida $[G : C_G(x_i)]$ per ogni $i = 1, \dots, t$. Dall'equazione delle classi ricaviamo che p divide $|Z(G)|$. Per il lemma di Cauchy nel caso abeliano, esiste un elemento $z \in Z(G)$ tale che il sottogruppo $A = \langle z \rangle$ ha ordine p. Inoltre per il lemma 5.72 A è normale in G e $|G/A| = |G|/p$. Pertanto la massima potenza di p che divide $|G/A|$ è p^{a-1} e per l'ipotesi induttiva esiste un sottogruppo $\overline{H}$ di G/A di ordine p^{a-1}. Per il teorema di corrispondenza esiste un sottogruppo H di G che contiene A tale che $\overline{H} = \pi(H)$, se π è la proiezione canonica di G su G/A. Per il teorema di Lagrange 5.52 $|H| = [H : A]|A| = |H/A||A| = p^{a-1}p = p^a$, che conclude la dimostrazione. □

Osserviamo che se H è un sottogruppo di G, in generale H non è normale in G, ma potrebbe essere normale in un altro sottogruppo più piccolo di G. Per esempio H risulta sempre normale in H stesso. Consideriamo pertanto il più grande di questi sottogruppi.

Definizione 8.18. Sia G un gruppo e X un sottoinsieme di G. Un elemento g *normalizza* X se $X^g = X$. L'insieme $N_G(X) = \{g \in G : X^g = X\}$ degli elementi di G che normalizzano X si chiama il *normalizzante di X in G*.

Come per il centralizzante di un sottoinsieme di G, esaminiamo alcune semplici proprietà del normalizzante.

Lemma 8.19. *Siano G un gruppo e H un sottogruppo di G. Allora:*

(a) $N_G(H)$ è un sottogruppo di G;
(b) H è un sottogruppo normale di $N_G(H)$;
(c) $N_G(H)$ è il più grande sottogruppo di G in cui H è normale.

DIMOSTRAZIONE. (a) Osserviamo che se $xH = Hx$, moltiplicando a destra e a sinistra per x^{-1}, otteniamo $Hx^{-1} = x^{-1}H$, da cui si ricava immediatamente che $x^{-1} \in N_G(H)$. Se ora $x, y \in N_G(H)$, allora

$$(xy)H = x(yH) = x(Hy) = (xH)y = (Hx)y = H(xy).$$

Quindi $xy \in N_G(H)$.

(b) Se $h \in H$, allora $hH = Hh$ per la proprietà di chiusura del sottogruppo. Pertanto $h \in N_G(H)$, cioè $H \leq N_G(H)$. Il fatto che H sia normale in $N_G(H)$ viene direttamente dalla definizione.

(c) Sia ora K un sottogruppo di G tale che H è normale in K. Sia dunque $k \in K$; allora $kH = Hk$, cioè $k \in N_G(H)$ per la definizione di normalizzante. □

Il seguente lemma permette di calcolare il numero di coniugati di un sottogruppo H tramite il normalizzante di H.

Lemma 8.20. *Sia H un sottogruppo del gruppo G. Allora il numero dei coniugati di H coincide con l'indice del normalizzante di H in G.*

DIMOSTRAZIONE. Vogliamo dimostrare che

$$|\{H^g : g \in G\}| = [G : N_G(H)].$$

Ricordando che vale

$$[G : N_G(H)] = |\{N_G(H)g : g \in G\}|,$$

costruiamo una biezione tra questi due insiemi. Siano $N = N_G(H)$ e

$$f : \{Ng : g \in G\} \to \{H^g : g \in G\} \quad \text{definita da} \quad f(Ng) = H^g \ \forall g \in G.$$

Dimostriamo che f è ben definita e che è iniettiva:

$$Ng = Nx \iff gx^{-1} \in N \iff (xg^{-1})H(gx^{-1}) = H \iff$$

$$g^{-1}Hg = x^{-1}Hx \iff f(Ng) = f(Nh).$$

Infine f è suriettiva per costruzione. □

8.3 Semplicità di A_n

In questa sezione vogliamo dimostrare che i gruppi alterni A_n sono gruppi semplici non abeliani, per ogni $n \geq 5$. Dimostriamo dapprima una proposizione.

Proposizione 8.21. *Se $n \geq 3$, ogni elemento di A_n è prodotto di 3-cicli.*

DIMOSTRAZIONE. Se $\sigma = id$, allora $\sigma = (123) \circ (123) \circ (123)$. Sia $\sigma \neq id$ un elemento di A_n; allora σ si può scrivere come prodotto di un numero pari di trasposizioni $\sigma = (a_{11}a_{12}) \circ (a_{21}a_{22}) \circ \ldots \circ (a_{t1}a_{t2})$. Se si dimostra che il prodotto di ogni coppia di trasposizioni è il prodotto di 3-cicli, si conclude che ogni permutazione pari è il prodotto di 3-cicli. Sia dunque $(ab) \circ (cd)$ prodotto di due trasposizioni.

Se $\{a, b\} = \{c, d\}$, allora $(ab) \circ (cd) = id$ è prodotto di 3-cicli.

Se $\{a, b\} \cap \{c, d\} = \{b\}$, per esempio $b = c$, allora

$$(ab) \circ (cd) = (ab) \circ (bd) = (abd).$$

Se $\{a, b\} \cap \{c, d\} = \emptyset$, allora

$$(ab) \circ (cd) = (ab) \circ (bc) \circ (bc) \circ (cd) = (abc) \circ (bcd).$$

□

In generale non è facile capire quando due elementi di un gruppo sono coniugati. Nel caso dei gruppi simmetrici però c'è un utile criterio per riconoscere quando due permutazioni sono coniugate.

Lemma 8.22. *Siano $(a_1 \ldots a_d)$ un ciclo in S_n e $\sigma \in S_n$. Allora il coniugato di $(a_1 \ldots a_d)$ tramite σ^{-1} è l'elemento $(\sigma(a_1) \ldots \sigma(a_d))$.*

DIMOSTRAZIONE. Ricordando la definizione di ciclo come applicazione biettiva dell'insieme $\{1, 2, \ldots, n\}$ in se stesso, dimostriamo che l'applicazione $(a_1 \ldots a_d)^{\sigma^{-1}}$ coincide con l'applicazione $(\sigma(a_1) \ldots \sigma(a_d))$. Denotiamo con f il ciclo $(a_1 \ldots a_d)$. Poniamo $b_i := \sigma(a_i)$ per ogni $i = 1, \ldots, n$, chiaramente si ha anche $a_i = \sigma^{-1}(b_i)$. Allora

$$f(\sigma^{-1}(b_i)) = f(a_i) = a_{i+1} \quad \text{se } i = 1, 2, \ldots, d-1$$
$$\text{e } f(\sigma^{-1}(b_d)) = f(a_d) = a_1,$$

da cui

$$(\sigma \circ f \circ \sigma^{-1})(b_i) = \sigma(f(\sigma^{-1}(b_i))) = \sigma(a_{i+1}) = b_{i+1} \text{ per } i = 1, \ldots, d-1 \text{ e}$$
$$(\sigma \circ f \circ \sigma^{-1})(b_d) = b_1.$$

Da questo si ricava che $(\sigma \circ f \circ \sigma^{-1})$ agisce sull'insieme $\{b_1, \ldots, b_d\}$ esattamente come il ciclo

$$(b_1, \ldots, b_d) = (\sigma(a_1) \ldots \sigma(a_d)).$$

Sia $j \notin \{b_1, \ldots, b_d\}$; allora

$$j \notin \sigma(\{a_1, \ldots, a_d\})$$

e quindi $\sigma^{-1}(j) \notin \{a_1, \ldots, a_d\})$. Pertanto per ogni $j \notin \{b_1, \ldots, b_d\}$, si ha

$$(\sigma \circ f \circ \sigma^{-1})(j) = \sigma(f(\sigma^{-1}(j))) = \sigma(\sigma^{-1}(j)) = j.$$

□

Osserviamo che se $(a_1 \ldots a_d)$ e $(b_1 \ldots b_d)$ sono cicli della stessa lunghezza d in S_n, esiste una permutazione σ tale che $(a_1 \ldots a_d)^\sigma = (b_1 \ldots b_d)$. È sufficiente prendere σ con

$$\sigma(b_i) = a_i \quad \text{per ogni } i = 1, \ldots, d.$$

Pertanto tutti i cicli della stessa lunghezza sono coniugati in S_n. In generale non è detto però che questo avvenga anche in A_n, come si vede dal seguente esempio.

Esempio 8.23. Siano $\sigma = (12345)$ e $\rho = (12435)$ due cicli di S_5. Poiché σ e ρ sono permutazioni pari, appartengono entrambi ad A_5. Per il lemma 8.22 σ e ρ sono coniugati in S_5, per esempio tramite $\tau = (34)$. Per l'esercizio 8.17 non c'è nessuna permutazione $\alpha \in A_5$ tale che $\sigma^\alpha = \rho$.

Il seguente lemma 8.24 garantisce che, nel caso particolare dei 3-cicli, questo avviene anche in A_n.

Lemma 8.24. *Sia $n \geq 5$, allora i 3-cicli formano un'unica classe di coniugio in A_n.*

DIMOSTRAZIONE. Siano $\sigma = (abc)$ e τ due 3-cicli in A_n. Allora esiste una permutazione $\psi \in S_n$ tale che $\sigma^\psi = \tau$. Se $\psi \in A_n$, allora σ e τ sono coniugati anche in A_n. Poiché $n \geq 5$, esistono due elementi d, e tali che $\{a, b, c\} \cap \{d, e\} = \emptyset$. Se $\psi \notin A_n$, la permutazione ψ è dispari e quindi la permutazione $\alpha = (de)\psi$ è pari e appartiene ad A_n. Inoltre

$$\sigma^\alpha = (\sigma^{(de)})^\psi = \sigma^\psi = \tau$$

che prova che σ e τ sono coniugate anche in A_n. □

Se

$$\rho = (a_{11} \dots a_{1d_1}) \dots (a_{n1} \dots a_{nd_n})$$

è la decomposizione in cicli disgiunti di una permutazione ρ, chiameremo la n-upla non ordinata $(d_1, d_2, \dots, d_n)$ *struttura ciclica* di ρ. Come conseguenza del lemma 8.22, si ha che la struttura ciclica viene preservata dal coniugio. Infatti, $\rho^{\sigma^{-1}}$ ha la stessa struttura ciclica in quanto

$$\begin{aligned}\rho^{\sigma^{-1}} &= ((a_{11} \dots a_{1d_1}) \dots (a_{n1} \dots a_{nd_n}))^{\sigma^{-1}} = \\ &= (a_{11} \dots a_{1d_1})^{\sigma^{-1}} \dots (a_{n1} \dots a_{nd_n})^{\sigma^{-1}} = \\ &= (\sigma(a_{11}) \dots \sigma(a_{1d_1})) \dots (\sigma(a_{n1}) \dots \sigma(a_{nd_n})).\end{aligned}$$

D'altra parte sia ρ' un'altra permutazione con struttura ciclica dello stesso tipo $(d_1, d_2, \dots, d_n)$, cioè ρ' è uguale al prodotto di cicli disgiunti

$$\rho' = (b_{11} \dots b_{1d_1})(b_{21} \dots b_{2d_2}) \dots (b_{n1} \dots b_{nd_n}).$$

Allora possiamo facilmente definire una permutazione σ tale che $\sigma(a_{ij}) = b_{ij}$ per tutti i possibili i, j. Allora è chiaro che $\rho' = \rho^{\sigma^{-1}}$. Abbiamo così dimostrato la seguente proposizione.

Proposizione 8.25. *Due permutazioni sono coniugate se e solo se hanno la stessa struttura ciclica.*

Ci proponiamo di dimostrare che il gruppo alterno A_n è un gruppo semplice non abeliano. Per far questo utilizzeremo la seguente proposizione.

Proposizione 8.26. *Sia N un sottogruppo normale proprio di S_n, $n \geq 3$. Allora $N = \{1\}$ o $N = A_n$.*

DIMOSTRAZIONE. Sia N sottogruppo normale di S_n e supponiamo $N \cap A_n \neq \{id\}$. Sia $id \neq \sigma \in N \cap A_n$; allora per l'esercizio 8.9 esiste una trasposizione τ tale che $[\sigma, \tau] \neq id$. Poiché N è normale in S_n, dall'osservazione 8.2 si ha $[\sigma, \tau] \in N$. Inoltre $[\sigma, \tau] = (\tau^{-1})^\sigma \circ \tau$ è un prodotto di trasposizioni non identico. Allora $[\sigma, \tau]$ è un prodotto di due trasposizioni disgiunte oppure un 3 ciclo, se

$$|\text{supp}((\tau^{-1})^\sigma) \cap \text{supp}(\tau)| = 1.$$

Pertanto $N \cap A_n$ contiene o un 3-ciclo o il prodotto di due trasposizioni disgiunte e poiché $N \cap A_n \trianglelefteq A_n$, ne contiene tutti i coniugati. Dal fatto che A_n è generato dai 3-cicli, per $n \geq 3$, o dai prodotti di coppie di trasposizioni disgiunte, se $n \geq 4$, segue che $N \geq A_n$. Possiamo pertanto supporre $N \cap A_n = \{id\}$. Allora

$$2 \geq |NA_n/A_n| = |N/N \cap A_n| = |N|$$

e quindi N è un sottogruppo normale di S_n con $|N| \leq 2$. Per l'esercizio 8.5 si avrebbe $N \leq Z(S_n)$. Essendo $Z(S_n) = \{id\}$ per l'esercizio 8.3, concludiamo che $N = \{id\}$. □

Siamo ora in grado di dimostrare il seguente teorema.

Teorema 8.27. *Per $n \geq 5$, il gruppo alterno A_n è semplice non abeliano.*

DIMOSTRAZIONE. Sia τ una qualsiasi trasposizione di S_n. Allora $S_n = \langle A_n, \tau \rangle$. Sia N un sottogruppo normale non banale di A_n. Poiché A_n è normale in S_n, allora N^τ è contenuto in A_n ed è normale in A_n. Consideriamo il normalizzante $N_{S_n}(N)$ di N; poiché N è normale in A_n si ha $N_{S_n}(N) \geq A_n$. Se $N_{S_n}(N) = S_n$, allora il lemma 8.26 permette di concludere che $N = A_n$. Se $N_{S_n}(N) = A_n$, allora per il lemma 8.20 il numero di coniugati di N è esattamente $[S_n : A_n] = 2$. Pertanto se τ è una trasposizione, allora $\tau \notin A_n$ e quindi τ non normalizza N, da cui

$$N \cap N^\tau < N \quad \text{e} \quad NN^\tau > N.$$

D'altro canto $N^\tau \leq A_n$ e quindi $NN^\tau \leq A_n$. Per il lemma 8.7 il cuore e la chiusura normale di N in S_n sono dati rispettivamente da $N_{S_n} = N \cap N^\tau$ e $N^{S_n} = NN^\tau$. Poiché N_{S_n} è normale in S_n ed è strettamente contenuto in A_n, per la proposizione 8.26 si ha $N_{S_n} = N \cap N^\tau = \{id\}$. Analogamente si prova

$$N^{S_n} = NN^\tau = A_n.$$

Per il teorema 6.35 A_n è isomorfo al prodotto diretto dei suoi due sottogruppi normali N ed N^τ. Allora

$$|A_n| = |N||N^\tau| = |N|^2.$$

Poiché $n \geq 5$, 2 divide $|A_n|$, allora 2 divide $|N|$. Per il lemma di Cauchy 8.12 esiste un elemento di ordine 2 in N, cioè esiste σ di ordine 2. Se scriviamo σ come prodotto di cicli disgiunti, per l'esercizio 5.10 ciascuno di questi cicli deve avere ordine 2. Pertanto $\sigma = \tau_1 \dots \tau_r \in N$, con τ_i trasposizioni disgiunte per $i = 1, \dots, r$. Ma allora

$$id \neq \sigma^{\tau_1} = \sigma \in N \cap N^{\tau_1},$$

in contraddizione con $N \cap N^{\tau_1} = \{id\}$. □

Utlizzando il teorema 8.27 si può dimostrare che esiste un gruppo infinito isomorfo a $\bigcup_{n \in \mathbb{N}_+} A_n$ che risulta essere semplice non abeliano, si veda l'esercizio 8.4.

8.4 Azioni di gruppi e teoremi di Sylow

In questa sezione dimostriamo i teoremi di Sylow per i gruppi finiti. Nell'esercizio 8.21 si prova che dato un divisore dell'ordine di un gruppo finito G non sempre esiste un sottogruppo di quell'ordine. Il lemma di Cauchy 8.12 garantisce che se il divisore è un primo p allora esiste un sottogruppo di ordine p. Il primo teorema di Sylow 8.17 asserisce che se p^n è la massima potenza di p che divide l'ordine del gruppo, allora esiste un sottogruppo esattamente di quell'ordine.

Gli altri due teoremi di Sylow affermano che tutti i p-sottogruppi di Sylow sono a due a due coniugati e danno delle informazioni sul numero dei p-sottogruppi di Sylow. Non daremo qui la dimostrazione originaria di Sylow, ma una dimostrazione successiva dovuta a Wielandt che fa uso delle azioni di gruppo. Poiché il concetto di azione di gruppo è in ogni caso molto importante, lo introduciamo ora.

Definizione 8.28. Sia G un gruppo e Ω un insieme non vuoto. Diciamo che G *agisce su* Ω tramite f o che f definisce un'*azione di* G *su* Ω se esiste un omomorfismo $f : G \to S_\Omega$. Denotiamo con $g.x$ l'immagine $f(g)(x)$ di x tramite la biezione $f(g)$. Inoltre $\ker f$ si dice il *nucleo dell'azione* e l'azione si dice *fedele* se $\ker f = \{1\}$. Se f è l'omomorfismo banale che manda ogni elemento di G nell'identità allora l'azione si dice *banale*.

Un altro modo per vedere le azioni in modo forse meno formale è il seguente.

Sia G un gruppo e Ω un insieme non vuoto. Un'*azione di* G *su* Ω è un'applicazione $\varphi : G \times \Omega \to \Omega$ tale che, se denotiamo con gx l'elemento $\varphi(g, x)$ valgono

(a) $(g_1g_2)x = g_1(g_2x)$ per ogni $g_1, g_2 \in G$ e per ogni $x \in \Omega$;
(b) $1x = x$ per ogni $x \in \Omega$.

Non è difficile vedere che le due definizioni di azioni di un gruppo su un insieme si determinano reciprocamente, si veda l'esercizio 8.31.

Vediamo ora alcuni esempi.

Esempio 8.29. Siano Ω insieme non vuoto e G un sottogruppo di S_Ω. Allora l'applicazione $\varphi : G \times \Omega \to \Omega$ definita da $\varphi(\sigma, x) = \sigma(x)$ per ogni $\sigma \in G, x \in \Omega$ definisce un'azione di G su Ω, detta *azione naturale di G su* Ω.

Esempio 8.30. Sia G un sottogruppo del gruppo lineare $GL_n(K)$, con $n \in \mathbb{N}_+$ e K campo. Sia V uno spazio vettoriale di dimensione n su K e denotiamo con $A \cdot v$ la moltiplicazione righe per colonne della matrice $A \in GL_n(K)$ e del vettore colonna $v \in V$. L'applicazione $\varphi : G \times V \to V$ definita da $\varphi(A, v) = A \cdot v$ per ogni $A \in G, v \in V$, definisce un'azione fedele di G su V, che viene chiamata *azione naturale di G su V*.

Nel caso in cui $n = 1$, si ottiene un'azione di K^* su K per moltiplicazione.

Esempio 8.31. Consideriamo la retta reale $\mathbb{R}$ e il gruppo

$$G = \{f : \mathbb{R} \to \mathbb{R} \text{ definita da } f(x) = ax + b, \forall x \in \mathbb{R};\ a, b \in \mathbb{R}, a \neq 0\},$$

come definito nell'esercizio 4.16. Allora l'applicazione $\varphi : G \times \mathbb{R} \to \mathbb{R}$ con $\varphi(f, x) = f(x)$ definisce un'azione di G su $\mathbb{R}$

Vediamo altri esempi di azioni, in cui l'insieme Ω su cui agisce il gruppo G è l'insieme supporto G del gruppo stesso.

Esempio 8.32. Nel teorema di Cayley 6.27 è definita un'azione di un qualsiasi gruppo $(G, \cdot)$ sull'insieme G per *moltiplicazione a sinistra*. Quest'azione è fedele.

Esempio 8.33. Possiamo definire un'azione del gruppo $(G, \cdot)$ sull'insieme G *per coniugio*. Nel teorema 6.26 si costruisce infatti un omomorfismo f di G in $\mathrm{Aut}(G)$, sottogruppo di S_G, ponendo $f(g)$ il coniugio tramite g^{-1}. In questo caso si dice che G agisce su se stesso per coniugio e il nucleo dell'azione è il centro di G.

Sia G un gruppo che agisce su un insieme Ω tramite f. Definiamo una relazione $\sim_G$ in Ω, ponendo

$$x \sim_G y \quad \text{se e solo se esiste} \quad g \in G \quad \text{tale che} \quad f(g)(x) = y.$$

Si verifica che $\sim_G$ è una relazione di equivalenza, si veda l'esercizio 8.30. Allora le classi di equivalenza rispetto alla relazione $\sim_G$ costituiscono una partizione.

Definizione 8.34. Siano G un gruppo che agisce su un insieme Ω e $x \in \Omega$. Allora la classe di equivalenza $[x]_{\sim_G} = \{g.x : g \in G\}$ si chiama *orbita di x tramite f* e si denota anche con $\mathcal{O}_x$.

L'insieme delle orbite è una partizione. Se in Ω esiste una sola orbita, allora G si dice *transitivo*. Dalla definizione, un gruppo G che agisce su Ω è transitivo se e solo se per ogni $x, y \in \Omega$ esiste $g \in G$ tale che $g.x = y$.

L'insieme $G_x = \{g \in G : g.x = x\}$ si dice *stabilizzatore di x*.

Denotiamo con Ω_G l'insieme dei *punti fissi* di G in Ω, cioè

$$\Omega_G = \{x \in \Omega : g.x = x \ \text{ per ogni } g \in G\}.$$

Osserviamo che un'orbita Δ ha cardinalità 1 se e solo se $\Delta = \{x\}$ e $g.x = x$ per ogni $g \in G$, cioè se e solo se $x \in \Omega_G$.

Esempio 8.35. Siano G un gruppo, H un sottogruppo di G e $\Omega = \{xH : x \in G\}$. Allora G agisce su Ω tramite $f : G \to S_\Omega$ definita da $f(g)(xH) = gxH$. Infatti $f(g)$ è iniettiva perché $gxH = gyH$ implica $xH = yH$ e $f(g)$ è suriettiva perché data $xH \in \Omega$, si ha $f(g)(g^{-1}xH) = xH$. Allora $f(g) \in S_\Omega$. Mostriamo che f è un omomorfismo:

$$f(gk)(xH) = gkxH = f(g)(kxH) = f(g)(f(k)(xH)) = (f(g) \circ f(h))(xH).$$

Quest'azione si chiama *azione per moltiplicazione a sinistra sulle classi laterali sinistre di H*. Il nucleo dell'azione è

$$\ker f = \{g \in G : gxH = xH \quad \text{per ogni} \quad x \in G\},$$

cioè $g \in \ker f$ se e solo se $g \in xHx^{-1}$ per ogni $x \in G$. Allora il nucleo dell'azione è esattamente il cuore H_G di H in G.

Se $H = \{1\}$, si ottiene l'azione μ definita nel teorema di Cayley 6.27.

In modo analogo si può definire un'azione su $\Omega = \{Hx : x \in G\}$, tramite $f : G \to S_\Omega$ definita da $f(g)(Hx) = Hxg^{-1}$. Quest'azione si chiama *azione per moltiplicazione a destra sulle classi laterali destre di* H.

Dimostriamo ora un lemma che mette in relazione le orbite di un'azione e gli stabilizzatori.

Lemma 8.36. *Siano* G *un gruppo che agisce su un insieme* Ω *tramite* f *e* $x \in \Omega$. *Lo stabilizzatore* G_x *di* x *è un sottogruppo di* G *e se* $\mathcal{O}_x$ *è l'orbita di* x *rispetto ad* f, *allora*

$$|\mathcal{O}_x| = [G : G_x].$$

DIMOSTRAZIONE. Siano $g, h \in G_x$. Osserviamo che $1 \in G_x$. Poiché $f(g)$ lascia fisso x, anche la sua inversa $f(g)^{-1} = f(g^{-1})$ lascia fisso x, che prova che $g^{-1} \in G_x$. Inoltre

$$(gh).x = g.(h.x) = g.x = x,$$

che prova che G_x è un sottogruppo.

Sia $\mathcal{C}$ l'insieme delle classi laterali sinistre di G_x in G. Definiamo $\alpha : \mathcal{C} \to \mathcal{O}_x$ con $\alpha(gG_x) = g.x$ per ogni $g \in G$. Dimostriamo che α è ben definita e iniettiva:

$$gG_x = hG_x \iff h^{-1}g \in G_x \iff (h^{-1}g).x = x \iff$$

$$g.x = h.x \iff \alpha(gG_x) = \alpha(hG_x).$$

Dalla definizione di $\mathcal{O}_x$ segue che α è suriettiva. Pertanto α è una biezione e quindi gli insiemi $\mathcal{C}$ e $\mathcal{O}_x$ hanno la stessa cardinalità. Si conclude osservando che

$$|\mathcal{C}| = [G : G_x].$$

□

Sia G un gruppo che agisce su se stesso per coniugio come nell'esempio 8.33; allora lo stabilizzatore di un elemento $x \in G$ è il centralizzante $C_G(x)$ e applicando il lemma 8.36 si ottiene la proposizione 8.11.

Vediamo qualche altro esempio.

Esempio 8.37. A partire da un'azione di un gruppo G su un insieme Ω, possiamo costruire un'azione di G sull'insieme $\mathcal{P}(\Omega)$ nel modo seguente. Se $f : G \to S_\Omega$ definisce un'azione di G su Ω e poniamo $f(g)(x) = g.x$, definiamo allora

$$\varphi : G \to S_{\mathcal{P}(\Omega)} \quad \text{con} \quad \varphi(g)(X) = g.X = \{g.x : x \in X\}$$

per ogni $g \in G$ e $X \in \mathcal{P}(\Omega)$. Allora $\varphi(g)$ è ben definita ed è iniettiva perché se $g.X = g.Y$, questo implica che per ogni $x \in X$, esiste $y \in Y$ tale che $g.x = g.y$, da cui $x = y$ e quindi $X \subseteq Y$. L'altra inclusione si dimostra in modo analogo. Inoltre

$\varphi(g)$ è suriettiva, infatti per ogni $X \in \mathcal{P}(\Omega)$, esiste $Y = \{g^{-1}.x : x \in X\}$ con $g.Y = X$. Infine φ è un omomorfismo e pertanto definisce un'azione.

Possiamo restringere tale azione ai sottoinsiemi di cardinalità n di Ω, come segue. Per ogni $n \in \mathbb{N}$ sia

$$[\Omega]^n = \{X \in \mathcal{P}(\Omega) : |X| = n\};$$

allora la restrizione dell'azione di G su $\mathcal{P}(\Omega)$ all'insieme $[\Omega]^n$ definisce un'azione di G su $[\Omega]^n$, in quanto $|X| = |g.X|$.

Consideriamo ad esempio l'azione di un gruppo G su se stesso per coniugio definita nell'esempio 8.33 e la relativa azione di G su $\mathcal{P}(G)$. Allora lo stabilizzatore di un sottoinsieme X di G è esattamente il suo normalizzante $N_G(X)$ come definito in 8.18.

Analogamente si ha un'azione per coniugio di G nel reticolo $\mathcal{L}(G)$ dei sottogruppi di G. Allora il lemma 8.19 è ora un corollario del lemma 8.36.

Esaminiamo il caso in cui il gruppo che agisce su un insieme finito sia un p-gruppo finito, p un primo. Otteniamo un'utile relazione tra la cardinalità dell'insieme e quella dell'insieme dei suoi punti fissi.

Lemma 8.38. *Siano G un p-gruppo finito, p un primo, che agisce su un insieme finito Ω e Ω_G l'insieme dei punti fissi di G in Ω. Allora*

$$|\Omega| \equiv_p |\Omega_G|.$$

DIMOSTRAZIONE. Osserviamo che Ω è l'unione disgiunta delle orbite di G. Possiamo suddividere le orbite a seconda della loro cardinalità. Abbiamo osservato che un'orbita Δ ha cardinalità 1 se e solo se $x \in \Omega_G$. Inoltre se un'orbita Δ ha cardinalità maggiore di 1, si ha che, se $x \in \Delta$,

$$|\Delta| = |\mathcal{O}_x| = [G : G_x] = p^r$$

per qualche $r \in \mathbb{N}_+$. Se denotiamo con Δ_i, per $i = 1, \ldots, t$ le orbite di cardinalità maggiore di 1, si ha:

$$|\Omega| = |\Omega_G| + |\Delta_1| + \ldots + |\Delta_t| \equiv_p |\Omega_G|,$$

poiché le orbite costituiscono una partizione di Ω. □

Se consideriamo l'azione di un gruppo finito G su se stesso per coniugio, allora l'insieme dei punti fissi rispetto a quest'azione è il centro di G. Pertanto se G è un p-gruppo finito, p primo, si può ricavare la conclusione del lemma 8.14 dal lemma 8.38.

Si può dare una dimostrazione alternativa al primo teorema di Sylow 8.17, utilizzando i risultati fin qui provati sulle azioni di gruppo; si veda l'esercizio 8.43.

Il primo teorema di Sylow 8.17 dimostra l'esistenza di p-sottogruppi di Sylow per ogni gruppo finito di ordine divisibile per p, p primo. Se un sottogruppo è coniugato ad un p-sottogruppo di Sylow, allora è anch'esso un p-sottogruppo di Sylow. Dimostriamo che tutti i p-sottogruppi di Sylow sono coniugati.

Teorema 8.39. *Siano G un gruppo finito di ordine divisibile per p, p primo, P un p-sottogruppo di G e $S \in Syl_p(G)$. Allora esiste $g \in G$ tale che $P \leq S^g$.*

DIMOSTRAZIONE. Sia $\Omega = \{xS : x \in G\}$. Facciamo agire P su Ω per moltiplicazione a sinistra, come descritto nell'esempio 8.35. Poiché $|\Omega| = [G : S]$, si ha che p non divide $|\Omega|$, in quanto $S \in Syl_p(G)$. Per il lemma 8.38 si ha

$$|\Omega_P| \equiv_p |\Omega| \not\equiv_p 0,$$

cioè l'insieme

$$\Omega_P = \{xS : gxS = xS \text{ per ogni } g \in P\}$$

non è vuoto. Sia $xS \in \Omega_P$; allora $gxS = xS$ per ogni $g \in P$, da cui $g \in xSx^{-1}$ per ogni $g \in P$. Questo dimostra che $P \leq S^{x^{-1}}$. □

Corollario 8.40. (Secondo teorema di Sylow) *Siano G un gruppo finito e $P, S \in Syl_p(G)$. Allora esiste $g \in G$ tale che $P = S^g$. Inoltre*

$$|Syl_p(G)| = [G : N_G(S)] \quad \textit{divide} \quad [G : S].$$

DIMOSTRAZIONE. Per il teorema 8.39 esiste $g \in G$ tale che $P \leq S^g$ e

$$|P| = |S^g| < \infty \Longrightarrow P = S.$$

Il secondo enunciato segue dal teorema 8.20 e dal fatto che

$$[G : S] = [G : N_G(S)][N_G(S) : S]$$

per l'esercizio 5.41. □

Concludiamo con il terzo teorema di Sylow che fornisce informazioni sul numero dei coniugati di un p-sottogruppo di Sylow.

Teorema 8.41. (Terzo teorema di Sylow) *Siano G gruppo finito e p un primo che divide $|G|$. Allora $|Syl_p(G)| \equiv_p 1$.*

DIMOSTRAZIONE. Per il primo teorema di Sylow 8.17 esiste $S \in Syl_p(G)$. Facciamo agire S per moltiplicazione a sinistra sull'insieme delle classe laterali sinistre

$$\Omega = \{xS : x \in G\},$$

come descritto nell'esempio 8.35. Allora per il lemma 8.38 si ha

$$|\Omega_S| \equiv_p |\Omega| = [G : S].$$

Sia $xS \in \Omega_S$; allora $gxS = xS$ per ogni $g \in S$, cioè $gx \in xS$ per ogni $g \in S$, da cui $S \leq xSx^{-1}$. Allora $xS \in \Omega_S$ se e solo se $x \in N_G(S)$ e quindi

$$|\Omega_S| = [N_G(S) : S] \quad \text{e} \quad |Syl_p(G)| = [G : N_G(S)]$$

per il corollario 8.40. Osserviamo che

$$[G:S] = [G:N_G(S)][N_G(S):S]$$

e che tutti questi indici sono coprimi con p. Concludiamo che

$$[G:S] = |\Omega| \equiv_p |\Omega_S| = [N_G(S):S].$$

Essendo $[N_G(S):S]$ coprimo con p possiamo dividere per $[N_G(S):S]$ ricavando

$$|Syl_p(G)| = [G:N_G(S)] \equiv_p 1.$$

□

Notazione. Denotiamo con $n_p(G)$ il numero dei sottogruppi di Sylow di G, cioè $n_p(G) = |Syl_p(G)|$.

Osservazione 8.42. Osserviamo che se S è un p-sottogruppo di Sylow di un gruppo finito G, con p un primo, allora $n_p(G) = [G:N_G(S)]$ divide $[G:S]$. Inoltre S è normale se e solo se $n_p(G) = 1$.

Grazie al terzo teorema di Sylow è possibile dimostrare che l'ordine di un gruppo finito può talvolta caratterizzare il gruppo stesso. Ad esempio si è visto che esiste un unico gruppo di ordine 15 nell'esercizio 7.23 ed è quello ciclico. Lo svolgimento dell'esercizio è abbastanza complesso e non può essere generalizzato ad altri gruppi di ordine prodotto di due primi distinti. Dimostriamo ora che esiste un unico gruppo di ordine 15 (a meno di isomorfismi), con una tecnica che può venire utilizzata in una situazione più generale, come faremo nel teorema 8.44.

Esempio 8.43. Sia G un gruppo di ordine 15; allora G è ciclico.

Infatti sia P un 5-sottogruppo di Sylow di G. Allora per l'osservazione 8.42 $n_5(G)$ divide $[G:P] = 3$ e $n_5(G) \equiv_5 1$ da cui segue che $n_5(G) = 1$ e che P è normale. Sia ora Q un 3-sottogruppo di Sylow; allora $n_3(G)$ divide $[G:Q] = 5$ e per il terzo teorema di Sylow 8.41

$$n_3(G) \equiv_3 1$$

da cui segue che $n_3(G) = 1$ e che Q è normale. Si ha $|P| = 5$ e $|Q| = 3$, pertanto sia P che Q sono ciclici di ordine rispettivamente 5 e 3. Inoltre per il teorema 6.36 G è isomorfo al prodotto diretto $P \times Q$ che è ciclico di ordine 15 per il teorema 6.42.

Si veda anche l'esercizio 8.33 per altri esempi. L'argomento utilizzato nell'esempio 8.43 per dimostrare che un p-sottogruppo di Sylow del gruppo G è normale è basato sul fatto che in quelle ipotesi $[G:P]$ è congruo a 1 modulo p se e solo se è 1. Possiamo pertanto provare un teorema più generale.

Teorema 8.44. *Siano G un gruppo di ordine pq con p e q primi, $p > q$, P un p-sottogruppo di Sylow di G e Q un q-sottogruppo di Sylow di G. Allora:*

(a) P è normale in G;
(b) se $p \not\equiv_q 1$, allora Q è normale in G e G è isomorfo ad un gruppo ciclico di ordine pq.

DIMOSTRAZIONE. (a) Sappiamo che $n_p(G)$ divide $[G : P] = q < p$ per l'osservazione 8.42 e per il terzo teorema di Sylow 8.41

$$n_p(G) \equiv_p 1.$$

Da queste due condizioni si deduce che $n_p(G) = 1$, da cui P è normale.

(b) Analogamente $n_q(G)$ divide $[G : Q] = p$ per l'osservazione 8.42 e per il terzo teorema di Sylow 8.41 $n_q(G) \equiv_q 1$. Dall'ipotesi $p \not\equiv_q 1$ segue che $n_q(G) = 1$ e quindi che Q è normale. Si ha $|P| = p$ e $|Q| = q$, pertanto sia P che Q sono ciclici di ordine rispettivamente p e q. Inoltre per il teorema 6.36 G è isomorfo al prodotto diretto $P \times Q$ che è ciclico di ordine pq per il teorema 6.42. □

Il terzo teorema di Sylow 8.41 può essere utile per trovare dei sottogruppi normali in un gruppo finito. Osserviamo infatti che se G è un gruppo finito e p è un primo che divide l'ordine di G, si ha $|Syl_p(G)| = 1$ se e solo se esiste un unico sottogruppo di Sylow S e S è normale in G.

Esempio 8.45. Sia G un gruppo di ordine 42. Allora G non è semplice. Consideriamo infatti S un 7-sottogruppo di Sylow di G. Si ha che $n_7(G)$ divide $[G : S] = 6$ e deve essere congruo ad 1 modulo 7. L'unica possibilità è che $n_7(G) = 1$, cioè S è normale in G ed ha ordine 7, quindi G non è semplice.

8.5 Esercizi sui gruppi non abeliani

Esercizio 8.1 Sia G un gruppo non abeliano di ordine 6, si provi che $G \cong S_3$.

Esercizio 8.2 Provare che il sottoinsieme H del gruppo $GL_2(\mathbb{F}_3)$ che consiste delle matrici della forma $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, $a \in \mathbb{F}_3^*$, $b \in \mathbb{F}_3$, è un sottogruppo di $GL_2(\mathbb{F}_3)$ isomorfo a S_3.

Esercizio 8.3 Si dimostri che il centro del gruppo simmetrico S_n è banale per ogni $n \geq 3$.

Esercizio 8.4 Sia $S_{\mathbb{N}}$ il gruppo delle permutazioni di $\mathbb{N}$ e sia

$$FS_{\mathbb{N}} = \{\sigma \in S_{\mathbb{N}} : |\text{supp}(\sigma)| < \infty\}.$$

(a) Dimostrare che $FS_{\mathbb{N}}$ è un sottogruppo di $FS_{\mathbb{N}}$.
(b) Dimostrare che l'insieme $A_{\mathbb{N}} = \{\sigma \in FS_{\mathbb{N}} : \sigma$ è il prodotto di un numero pari di trasposizioni $\}$ è un sottogruppo di $FS_{\mathbb{N}}$.

(c) Per ogni $n \in \mathbb{N}_+$ sia

$$B_n = \{\sigma \in FS_{\mathbb{N}} : \text{supp}(\sigma) \subseteq \{0, 1, \ldots, n-1\}\}.$$

Dimostrare che $B_i \subseteq B_j$ se $i \leq j$ e che $B_n \cong S_n$, il gruppo simmetrico su n elementi. Dimostrare inoltre che

$$FS_{\mathbb{N}} = \bigcup_{n \in \mathbb{N}_+} B_n.$$

(d) Per ogni $n \in \mathbb{N}_+$, sia $C_n = \{\sigma \in A_{\mathbb{N}} : \text{supp}(\sigma) \subseteq \{0, 1, \ldots, n-1\}\}$. Dimostrare che $A_{\mathbb{N}} = \bigcup_{n \in \mathbb{N}_+} C_n$ e dedurre che $A_{\mathbb{N}}$ è un gruppo semplice infinito.

Esercizio 8.5 Sia N un sottogruppo di ordine 2 normale nel gruppo G. Si dimostri che N è contenuto nel centro di G.

Esercizio 8.6 Siano G un gruppo e H un sottogruppo di G. Per ogni $x \in G$ denotiamo con H^x il sottogruppo coniugato $x^{-1}Hx$ di H. Dimostrare che:

(a) H^x contiene l'intersezione $H \cap Z(G)$, in particolare $H \cap Z(G)$ è contenuto nel cuore H_G di H;
(b) esistono gruppi G per i quali l'uguaglianza $H \cap Z(G) = H_G$ fallisce per qualche sottogruppo proprio H.

Esercizio 8.7 Siano G un gruppo e H, K sottogruppi di G, tali che $H \leq K$. Se H è caratteristico in K e K è caratteristico in G, allora H è caratteristico in G.

Esercizio 8.8 Provare che $Z(A_n) = \{1\}$, per $n \geq 4$.

Esercizio 8.9 Sia $\sigma \in A_n$, $n \geq 3$. Allora esiste una trasposizione τ tale che

$$[\sigma, \tau] \neq id.$$

Esercizio 8.10 Sia H un sottogruppo di un gruppo G. Provare che $N_G(H) = H$, se l'indice $[G : H]$ è primo e H non è normale.

Esercizio 8.11 Sia $H = \langle (123) \rangle$ il sottogruppo del gruppo alterno $G = A_4$. Calcolare $N_G(H)$, $C_G(H)$ e l'indice $[N_G(H) : C_G(H)]$.

Esercizio 8.12 Sia G un gruppo finito e sia H un sottogruppo proprio di G. Provare che l'insieme $\bigcup_{x \in G} H^x$ è un sottoinsieme proprio di G.

Esercizio 8.13 Provare che, se il gruppo G non è abeliano, allora il gruppo $\text{Aut}(G)$ non può essere ciclico.

Esercizio 8.14 Provare che non esiste un gruppo G tale che $\text{Aut}(G) \cong \mathbb{Z}$.

Esercizio 8.15 Sia $m > 1$ un intero dispari. Allora non esiste un gruppo G tale che $\text{Aut}(G) \cong \mathbb{Z}_m$.

Esercizio 8.16 Decomporre $(23)(432)(12)(13) \in S_4$ nel prodotto di cicli disgiunti. Dimostrare che S_4 è generato da $\{(12),(13),(14)\}$.

Esercizio 8.17 Siano $\sigma = (12345)$, $\rho = (12435)$ e $\tau = (34)$ cicli di S_5.

(a) Si verifichi che

$$\sigma^{\alpha^{-1}} = \rho \quad \text{se e solo se} \quad \alpha \in \{(34),(1245),(14)(235),(13)(254),(1532)\}.$$

(b) Sia $H = \langle\sigma\rangle$. Si provi che $C_{S_5}(H) = H$.
(c) Si descriva la classe laterale τH e si concluda che $\sigma^{\alpha^{-1}} = \rho$ se e solo se $\alpha \in \tau H$.

Esercizio 8.18 Dimostrare che S_4 è generato da $\{(12),(1234)\}$.

Esercizio 8.19 Si dimostri che esiste un omomorfismo $f : S_4 \to S_3$ tale che

$$\ker f = \{id, (12)(34), (13)(24), (14)(23)\}.$$

Si dica se tale omomorfismo è suriettivo.

Esercizio 8.20 Sia H il sottogruppo di S_4 generato dai cicli (1234) e (13). Dimostrare che $H \cong D_8$.

Esercizio 8.21 * Provare che il gruppo alterno A_4 non ha sottogruppi di ordine 6.

Esercizio 8.22 Siano σ e τ le permutazioni di S_9 definite rispettivamente come segue:

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 2\,3\,1\,5\,6\,4\,8\,9\,7 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 4\,5\,6\,7\,8\,9\,1\,2\,3 \end{pmatrix}.$$

(a) Si dimostri che $\sigma \circ \tau = \tau \circ \sigma$.
(b) Si trovi la decomposizione in cicli disgiunti di σ, τ e $\sigma \circ \tau$.
(c) Si calcoli l'ordine di σ, τ e $\sigma \circ \tau$.
(d) Sia H il sottogruppo di S_9 generato da σ e τ. H è ciclico? H è abeliano? Quanti elementi ha H?

Esercizio 8.23 Siano τ_1, τ_2 e τ_3 le tre trasposizioni del gruppo simmetrico S_3 e siano σ_1 e σ_2 i due cicli di lunghezza 3.

(a) Dimostrare che ci sono sei automorfismi interni di S_3 e che:
(a$_1$) ogni automorfismo interno φ_{τ_i}, $i = 1,2,3$ fissa la trasposizione τ_i e scambia tra loro sia le altre due trasposizioni sia i cicli σ_1 e σ_2;
(a$_2$) ogni automorfismo interno φ_{σ_i} fissa entrambi i cicli σ_1, σ_2 e scambia tra loro le trasposizioni τ_i senza lasciarne una fissa.
(b*) Dimostrare che ogni automorfismo di S_3 è interno.

Esercizio 8.24 Sia p un numero primo e sia G un gruppo di ordine p^n per qualche $n \in \mathbb{N}$. Dimostrare che per ogni divisore d di $|G|$ esiste un sottogruppo di G di ordine d.

Esercizio 8.25 Sia G il gruppo $GL_2(\mathbb{R})$. Dimostrare che:

(a) i sottoinsiemi

$$B_2^+ = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in GL_2(\mathbb{R}) : a, b \in \mathbb{R} \right\} \text{ e}$$

$$B_2^- = \left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \in GL_2(\mathbb{R}) : a, b \in \mathbb{R} \right\}$$

di G sono sottogruppi abeliani isomorfi entrambi a $(\mathbb{R}, +) \times (\mathbb{R}^*, \cdot)$;

(b) le matrici

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G, \quad \text{con } a, b, c, d \in \mathbb{Q}$$

formano un sottogruppo H di G isomorfo a $GL_2(\mathbb{Q})$;

(c) siano $r \in \mathbb{R}$ un numero irrazionale e

$$x = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \ y = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}, \ z = \begin{pmatrix} r^{-1} & 0 \\ 0 & 1 \end{pmatrix} \text{ e } u = \begin{pmatrix} r^{-1} & 0 \\ 0 & r \end{pmatrix}.$$

Allora

$$H \cap H^x \leq B_2^+, \quad H \cap H^y \leq B_2^-,$$
$$H \cap H^z \leq D_2 \text{ e } H \cap H^u \leq D_2,$$

dove

$$D_2 := \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in GL_2(\mathbb{R}) : a, b \in \mathbb{R} \right\};$$

(d) esistono matrici $x, y \in G$, tali che $H \cap H^x \cap H^y \leq Z(GL_2(\mathbb{R}))$.

Esercizio 8.26 Sia G il sottoinsieme del gruppo $GL_2(\mathbb{R})$ formato da tutte le matrici della forma $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Dimostrare che:

(a) G è un sottogruppo di $GL_2(\mathbb{R})$;

(b) il centro di G è dato dalla sola matrice identica;

(c) le matrici $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$, con a e b numeri razionali, formano un sottogruppo H di G;

(d) se N^+ è l'insieme delle matrici $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G$ e $H_1 = H \cap N^+$, allora esiste una matrice $z \in G$ tale che $H_1 \cap H_1^z = \{I_2\}$, dove I_2 è la matrice identica di G;

(e) esistono matrici $x, z \in G$, tali che $H \cap H^x \cap H^z = \{I_2\}$.

Esercizio 8.27 Sia G il gruppo $SL_2(\mathbb{R})$. Dimostrare che:

(a) $Z(G) = \{I_2, -I_2\}$;

(b) le matrici $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, con a, b, c e d numeri razionali, formano un sottogruppo H di G;

(c) esistono matrici $x, y \in G$ tali che $H \cap H^x \cap H^y = \{\pm I_2\}$, dove I_2 è la matrice identica di G;
(d) se N è un sottogruppo normale di G contenuto in H, allora N è contenuto nel centro di G.

Esercizio 8.28 Per le matrici $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ e $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ del gruppo $G = GL_2(\mathbb{R})$ verificare che $o(a) = 4$ e $o(b) = 3$, mentre $o(ab) = \infty$.

Esercizio 8.29 Sia G il gruppo $T_2^+(\mathbb{R})$ delle matrici triangolari superiori in $GL_2(\mathbb{R})$. Dimostrare che per il sottogruppo $H = GL_2(\mathbb{Q}) \cap G$ di G esistono matrici $x, y \in G$ tali che

$$H \cap H^x \cap H^y \leq Z(G).$$

Esercizio 8.30 Sia G un gruppo che agisce su un insieme Ω. Definiamo una relazione $\sim_G$ in Ω, ponendo $x \sim_G y$ se e solo se esiste $g \in G$ tale che $g.x = y$. Dimostrare che $\sim_G$ è una relazione di equivalenza.

Esercizio 8.31 Siano G un gruppo, Ω un insieme non vuoto e

$$\varphi : G \times \Omega \to \Omega$$

un'applicazione tale che, se denotiamo con gx l'elemento $\varphi(g, x)$ valgono:

(a) $(g_1 g_2)x = g_1(g_2 x)$ per ogni $g_1, g_2 \in G$ e per ogni $x \in \Omega$;
(b) $1x = x$ per ogni $x \in \Omega$.

Si dimostri che:

(a) l'applicazione $\psi_g : \Omega \to \Omega$ definita da $\psi_g(x) = \varphi(g, x) = gx$, per ogni $x \in \Omega$, $g \in G$ è una biezione di Ω;
(b) l'applicazione $f : G \to S_\Omega$ con $f(g) = \psi_g$ definisce un'azione di G su Ω, come dalla definizione 8.28.

Esercizio 8.32 Siano G un gruppo finito ed H e K sottogruppi di G. Si dica se le seguenti affermazioni sono vere o false, fornendo una breve dimostrazione o un controesempio:

(a) se $[G : H] = 3$ e $|G|$ è dispari, allora H è normale in G;
(b) se $[G : H] = p$, con p primo allora H è normale in G;
(c) se $[G : H] = p$, con p primo allora H è massimale in G, cioè non esiste nessun sottogruppo $K \leq G$ tale che $H < K < G$.

Esercizio 8.33 Sia G un gruppo di ordine $n = 33, 35, 45, 51, 65, 69, 77, 85, 87, 91, 95, 99$. Dimostrare che G è abeliano e dire per quali di questi interi n il gruppo G è necessariamente ciclico.

Esercizio 8.34 Sia p un numero primo tale che $p > 3$ e 3 non divide $p - 1$. Provare che ogni gruppo G di ordine $3p$ è ciclico.

Esercizio 8.35 Descrivere i p-sottogruppi di Sylow di A_4 per ogni primo p che divide $|A_4|$.

Esercizio 8.36 Descrivere i 5-sottogruppi di Sylow di A_5.

Esercizio 8.37 Trovare un p-sottogruppo di Sylow di $GL_2(\mathbb{F}_p)$.

Esercizio 8.38 Dimostrare che il gruppo $GL_2(\mathbb{F}_3)$ ha esattamente quattro 3-sottogruppi di Sylow.

Esercizio 8.39 Dimostrare che gruppi di ordine n, con $n = 6$, 20, 330, non sono semplici.

Esercizio 8.40 Dimostrare che un gruppo di ordine pq, con p e q primi non necessariamente distinti, non è semplice.

Esercizio 8.41 * Sia G un gruppo non abeliano di ordine n, con $91 \leq n \leq 100$ e $n \neq 96$. Dimostrare che G non è semplice.

Esercizio 8.42 * Siano $n \in \mathbb{N}_+$ e p un primo. Dimostrare che

(a) il gruppo S_n ha un p-sottogruppo di Sylow non banale se e solo se $n \geq p$.
(b) se $n < p^2$, allora il gruppo S_n ha un p-sottogruppo di Sylow abeliano. Mostrare con un esempio che se $n \geq p^2$ allora un p-sottogruppo di Sylow di S_n non è abeliano.

Esercizio 8.43 Dare una dimostrazione alternativa al primo teorema di Sylow 8.17, utilizzando i risultati sulle azioni di gruppo.

Esercizio 8.44 Siano G un gruppo infinito e $B \subseteq G$. Allora B si dice *grande a sinistra* se esistono $n \in \mathbb{N}_+$ ed elementi $g_1, g_2, \ldots, g_n$ di G tali che $G = \bigcup_{i=1}^{\infty} g_i B$; B si dice *piccolo a sinistra* se esistono elementi $g_1, g_2, \ldots, g_n, \ldots$ a due a due distinti del gruppo G tali che $g_n B \cap g_m B = \emptyset$ se $m \neq n$ (analogamente si introducono i concetti di *grande a destra* e *piccolo a destra*). Dimostrare che

(a) se B è tale che BB^{-1} non è grande a sinistra, allora B è piccolo a sinistra;
(b) se S è un sottoinsieme finito di G, allora S è piccolo a sinistra e piccolo a destra;
(c) se $f : G \to H$ è un omomorfismo suriettivo di gruppi e B è un sottoinsieme grande a sinistra di H, allora $f^{-1}(B)$ è grande a sinistra in G;
(d) se B_i è un sottoinsieme grande a sinistra di un gruppo G_i, con $i = 1, 2, \ldots, n$, allora $B_1 \times \ldots \times B_n$ è grande a sinistra in $G_1 \times \ldots \times G_n$.

Esercizio 8.45 Siano G un gruppo infinito e H sottogruppo di G. Utilizzando le definizioni di sottoinsieme grande e piccolo a sinistra (a destra) definite nell'esercizio 8.44, dimostrare che le seguenti condizioni sono equivalenti:

(a) H ha indice infinito;
(b) H non è grande a sinistra;
(c) H non è grande a destra;
(d) H è piccolo a sinistra.

(e) H è piccolo a destra.

Esercizio 8.46 Sia G un gruppo infinito che agisce su un insieme X.

(a) Se F è un insieme finito di X e $s \in X \setminus F$, allora $\{g \in G : g.s \notin F\}$ è infinito.
(b) Se $x, y \in X$, allora l'insieme $M_{x,y} = \{g \in G : y = g.x\}$ è non vuoto se e solo se $\mathcal{O}_x = \mathcal{O}_y$. In tal caso $|M_{x,y}| = |G_x| = |G_y|$.
(c) Sia $S \subseteq X$ un sottoinsieme finito di X. Allora $M = \{g \in G : S \cap g.S \neq \emptyset\}$ è finito se e solo se $|G_x| < \infty$ per ogni $x \in S$.
(d) Se $S \subseteq X$ è un sottoinsieme finito di X tale che $|G_x| < \infty$ per ogni $x \in S$, allora esistono elementi $g_1, g_2, \dots, g_n, \dots$ a due a due distinti del gruppo G tali che $(g_n.S) \cap (g_m.S) = \emptyset$ qualora $m \neq n$.
(e) Se S ed F sono insiemi finiti disgiunti di X, allora $A = \{g \in G : F \cap g.S = \emptyset\}$ è infinito.

9

Anelli e ideali

Nei primi due paragrafi diamo le definizioni essenziali, alcuni esempi e le leggi di cancellazione in un anello. Nel terzo paragrafo introduciamo il corpo dei quaternioni. I paragafi 4, 5 e 6 sono dedicati alle sottostrutture associate ad un anello: sottoanelli, ideali destri, sinistri e bilateri e l'anello quoziente. Nel settimo paragrafo vengono definiti gli ideali primi e gli ideali massimali di un anello commutativo e ne viene data una caratterizzazione attraverso l'anello quoziente. Segue il teorema di Krull, che garantisce l'esistenza di ideali massimali negli anelli commutativi unitari.

9.1 Definizioni ed esempi

Ricordiamo alcune delle definizioni date nel quarto capitolo.

Un *anello* è una terna $(A, +, \cdot)$ dove A è un insieme, $+$ e $\cdot$ sono operazioni binarie su A che verificano le seguenti proprietà:

(1) la coppia $(A, +)$ è un gruppo abeliano con elemento neutro che denoteremo con 0.
(2) l'operazione $\cdot$ è *associativa*, cioè $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per ogni a, b e c in A;
(3) vale la legge distributiva, cioè

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{e} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

per ogni a, b e c in A.

Se esiste un elemento 1 di A, tale che $1 \neq 0$ e $1 \cdot a = a \cdot 1 = a$ per ogni a in A, si dice che A è *unitario* e 1 si dice *unità* dell'anello.

Come abbiamo già visto nel paragrafo 4.2, l'unità 1 di A, se esiste, è unica. Infatti, se per qualche elemento e di A risulta $e \cdot a = a \cdot e = a$ per ogni a in A, allora $e = e \cdot 1 = 1$.

Definizione 9.1. Per un anello unitario A un elemento a si dice *invertibile* se esiste un elemento x in A con $a \cdot x = x \cdot a = 1$.

L'insieme $U(A)$ di tutti gli elementi invertibili di A forma un gruppo per l'operazione $\cdot$. L'unico elemento x determinato dalla proprietà $a \cdot x = x \cdot a = 1$ si dice *inverso* dell'elemento a e si indica di solito con a^{-1}.

Denoteremo con A^* l'insieme degli elementi non nulli di A.

Quando non sarà necessario specificare le operazioni $+$ e $\cdot$, scriveremo A al posto di $(A, +, \cdot)$ e scriveremo ab al posto di $a \cdot b$.

Dati due elementi $a, b \in A$ si dice che a e b *commutano* (o sono *permutabili*) se $ab = ba$.

Definizione 9.2. Un anello A si dice *commutativo* se per ogni a, b in A risulta

$$ab = ba.$$

Vediamo ora qualche esempio di anello.

Esempio 9.3. - Se $\mathbb{Z}$ è l'insieme dei numeri interi, la terna $(\mathbb{Z}, +, \cdot)$ è un anello.
- Se $\mathbb{Q}$ è l'insieme dei numeri razionali, la terna $(\mathbb{Q}, +, \cdot)$ è un anello.
- Se $\mathbb{R}$ è l'insieme dei numeri reali, la terna $(\mathbb{R}, +, \cdot)$ è un anello.
- Se $\mathbb{C}$ è l'insieme dei numeri complessi, la terna $(\mathbb{C}, +, \cdot)$ è un anello.
- Se $m > 1$ è intero e $\mathbb{Z}_m$ è l'insieme delle classi resto modulo m, allora la terna $(\mathbb{Z}_m, +, \cdot)$ è un anello.
- Se $M_n(\mathbb{R})$ è l'insieme di tutte le matrici $n \times n$ a coefficienti reali e 0_n è la matrice nulla, allora la terna $(M_n(\mathbb{R}), +, \cdot)$ è un anello.

$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Z}_m, +, \cdot)$ sono anelli commutativi, mentre $M_n(\mathbb{R})$ non è commutativo se $n > 1$, come abbiamo mostrato nell'esercizio 4.4.

Proviamo alcune semplici proprietà che valgono in tutti gli anelli. Ricordiamo che per il gruppo abeliano $(A, +)$ si definiscono i multipli nx per $x \in A$ e $n \in \mathbb{Z}$ con le proprietà:

(1) $mx + nx = (m + n)x$;
(2) $-(nx) = (-n)x$;
(3) $n(mx) = m(nx) = nmx$;
(4) $n(x + y) = nx + ny$.

Lemma 9.4. *Siano x, y elementi di un anello A e $n, m \in \mathbb{Z}$. Allora*

(a) $0x = x0 = 0$;
(b) $(-x)y = x(-y) = -xy$;
(c) $(nx)y = x(ny) = n(xy)$;
(d) $(nx)(my) = (mx)(ny) = (mn)xy$.

DIMOSTRAZIONE. (a) Si ha $0x = (0 + 0)x = 0x + 0x$ da cui, per la legge di cancellazione della somma, si ha $0x = 0$. Analogamente per l'altra uguaglianza.

(b) Dalla (a) risulta $0 = 0y = (x + (-x))y = xy + (-x)y$ da cui risulta che $-xy = (-x)y$. Analogamente si dimostra l'altra uguaglianza.

(c) Supponiamo dapprima che n sia positivo e procediamo per induzione. Il caso $n = 0$ è stato dimostrato nel punto (a). Supponiamo vero l'asserto nel caso $n - 1$. Allora

$$(nx)y = ((n-1)x + x)y = ((n-1)x)y + xy = (n-1)xy + xy = n(xy).$$

Analogamente per l'altra uguaglianza. Se invece $n < 0$, usando (b) e il caso n positivo si ottiene

$$(nx)y = (-(-nx))y = -((-n)x)y = -((-n)(xy)) = n(xy).$$

(d) Segue da (c). □

Per un anello $(A, +, \cdot)$ unitario e un elemento $x \in A$ poniamo $x^0 = 1_A$. Per $n \in \mathbb{N}$ intero positivo definiamo le potenze x^n come nel caso di un gruppo. Restano vere le formule $x^m x^n = x^{m+n}$ e $(x^m)^n = x^{mn}$ per ogni $x \in A$ e ogni $m, n \in \mathbb{Z}$. Se $x, y \in A$ sono elementi permutabili, allora $(xy)^n = x^n y^n$ e x^n e y^m sono permutabili per ogni $n, m \in \mathbb{Z}$.

9.2 Le leggi di cancellazione in un anello

Definizione 9.5. Un elemento non nullo $a \in A$ si dice *divisore sinistro dello zero*, se esiste $b \neq 0$ in A con $ab = 0$. Analogamente, si dice che a è *divisore destro dello zero* se esiste $b \neq 0$ in A con $ba = 0$.

Lemma 9.6. *Se $ab = ac$ in un anello A e $a \neq 0$ non è divisore sinistro dello zero, allora vale $b = c$.*

DIMOSTRAZIONE. Da $ab = ac$ abbiamo $a(b - c) = ab - ac = 0$. Poiché a non è divisore sinistro dello zero possiamo concludere che $b - c = 0$ e quindi $b = c$. □

Abbiamo dimostrato che se a non è divisore sinistro dello zero si può cancellare a a sinistra. D'altra parte, se si può sempre cancellare a a sinistra, allora a non è divisore sinistro dello zero. Infatti se $ac = 0$ per qualche c in A, allora da $ac = a0$ concludiamo $c = 0$, quindi a non è divisore sinistro dello zero. In altre parole, si può cancellare a a sinistra se e solo se a non è divisore sinistro dello zero. Analogamente si dimostra che si può cancellare a a destra se e solo se a non è divisore destro dello zero.

Definizione 9.7. Un elemento $a \in A$ si dice *nilpotente* se esiste un intero positivo n tale che $a^n = 0$.

Si osservi che se un elemento non nullo è nilpotente, allora è senz'altro un divisore dello 0, mentre il viceversa non è vero. Infatti in $\mathbb{Z}_6$ l'elemento $[3]_6$ è un divisore dello 0, in quanto $[2]_6 \cdot [3]_6 = [0]_6$, ma non è nilpotente perché $([3]_6)^n = [3]_6 \neq [0]_6$ per ogni n.

Ricordiamo altre definizioni, già date nel paragrafo 4.4, che utilizzeremo in questo capitolo:

- un anello unitario privo di divisori dello zero destri (o equivalentemente privo di divisori dello zero sinistri) si dice *integro*;
- un anello commutativo integro unitario si dice *dominio di integrità* o più semplicemente *dominio*;
- un anello in cui tutti gli elementi non nulli sono invertibili, cioè $A^* = U(A)$ si dice *anello con divisione* o *corpo*;
- un corpo commutativo si dice *campo*.

Lemma 9.8. *Sia a un elemento invertibile di un anello A. Allora a non è un divisore dello zero.*

DIMOSTRAZIONE. Se $ac = 0$, allora abbiamo

$$c = 1c = (a^{-1}a)c = a^{-1}(ac) = a^{-1}0 = 0.$$

Pertanto a non è divisore sinistro dello zero. Analogamente si vede che a non è divisore destro dello zero. □

Dal lemma 9.8 si deduce che ogni campo è un dominio. L'anello $\mathbb{Z}$ dimostra che il viceversa non è vero in generale. In un caso particolare, cioè quando il dominio è finito, si ha invece l'equivalenza.

Lemma 9.9. *Sia A un anello commutativo finito privo di divisori dello 0, allora A è un campo.*

DIMOSTRAZIONE. Dobbiamo dimostrare che esiste un elemento neutro per la moltiplicazione e che ogni elemento non nullo ha un inverso. Sia $a \neq 0$ un elemento di A. Consideriamo l'applicazione $\mu_a : A \to A$ definita da $\mu_a(b) = ba(= ab)$. Allora μ_a è un'applicazione iniettiva. Infatti $\mu_a(b) = \mu_a(c)$ se e solo se $ba = ca$, cioè se e solo se $(b - c)a = 0$ e poiché $a \neq 0$ per ipotesi e in A non ci sono divisori dello zero, si ottiene che $b - c = 0$, da cui $b = c$. Inoltre μ_a è anche suriettiva, perché A è finito. Esiste pertanto un elemento $e \in A$ tale che $ea = a$. Poiché A è commutativo, $ea = ae$. Verifichiamo che e è l'elemento identico di A. Sia $c \in A$, allora esiste $b \in A$ tale che $c = ba$. Si ha $ce = (ba)e = b(ae) = ba = c$ e quindi per la commutatività anche $ec = ce = c$ per ogni $c \in A$. Usando nuovamente la suriettività di μ_a, otteniamo che esiste un elemento $b \in A$ tale che $ba = e$, cioè $b = a^{-1}$ è l'inverso di a. □

9.3 Il corpo dei quaternioni

Questo paragrafo è dedicato al corpo dei quaternioni, che generalizzano i numeri complessi. I quaternioni furono inventati nel 1843 dal matematico irlandese William Rowan Hamilton (1805-1865).

L'insieme $\mathbb{H}$ dei quaternioni coincide con il prodotto cartesiano

$$\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^4.$$

Un quaternione $q \in \mathbb{H}$ è una quadrupla $(a, b, c, d) \in \mathbb{R}^4$ di numeri reali. L'insieme $\mathbb{H}$ risulta un gruppo abeliano rispetto all'operazione $+$ definita da

$$(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d'). \qquad (1)$$

In altre parole il gruppo $(\mathbb{H}, +)$ coincide con il prodotto diretto

$$(\mathbb{R}, +) \times (\mathbb{R}, +) \times (\mathbb{R}, +) \times (\mathbb{R}, +),$$

cioè il gruppo additivo dello spazio vettoriale $\mathbb{R}^4$. Definiamo il prodotto in $\mathbb{H}$ in un modo più complicato, che richiede un'altra forma dei quaternioni che ricorda i numeri complessi. Denotiamo il quaternione $(0, 1, 0, 0)$ con i, il quaternione $(0, 0, 1, 0)$ con j e infine usiamo k per denotare il quaternione $(0, 0, 0, 1)$. Scriviamo anche 1 per il quaternione $(1, 0, 0, 0)$ e 0 per il quaternione $(0, 0, 0, 0)$. Chiamiamo i, j e k *identità immaginarie*. I vettori $1, i, j$ e k dello spazio vettoriale $\mathbb{R}^4$ formano una base, pertanto ogni quaternione $q = (a, b, c, d)$ di $\mathbb{H}$ può essere scritto come combinazione lineare $q = a1 + bi + cj + dk$. Omettendo l'1, scriveremo in seguito $q = a + bi + cj + dk$. Con queste notazioni la somma (1) può essere scritta anche come $q+q' = (a+a')+(b+b')i+(c+c')j+(d+d')k$, dove $q' = a'+b'i+c'j+d'k$. Il prodotto dei quaternioni è dato dalla formula

$$\begin{aligned}(a + bi + cj + dk)(a' + b'i + c'j + d'k) &= \\ = (aa' - bb' - cc' - dd') &+ (ab' + ba' + cd' - dc')i + \\ +(ac' + ca' + db' - bd')j &+ (ad' + da' + bc' - cb')k.\end{aligned}$$

Non è difficile vedere che valgono le seguenti regole di moltiplicazione delle unità immaginarie:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i \quad \text{e} \quad ki = -ik = j. \qquad (2)$$

Chiameremo i quaternioni della forma $q' = r \in \mathbb{R}$, cioè $q' = (r, 0, 0, 0)$ *quaternioni reali*. Per un quaternione reale r vale

$$rq = ra + rbi + rcj + rdk \quad \text{per ogni} \quad q = a + bi + cj + dk.$$

In altre parole la moltiplicazione per r avviene allo stesso modo della moltiplicazione per uno scalare r nello spazio vettoriale $\mathbb{R}^4$. Lasciamo al lettore la verifica delle leggi associativa e distributiva, si veda anche l'esercizio 10.11. Poiché

$$1 \cdot q = q \cdot 1 = q$$

per ogni $q \in \mathbb{H}$, $(\mathbb{H}, +, \cdot)$ risulta un anello unitario. Da (2) segue che $\mathbb{H}$ non è commutativo.

Per un quaternione $q = a + bi + cj + dk$ poniamo $\overline{q} = a - bi - cj - dk$. Allora valgono le seguenti uguaglianze:

$$\overline{\overline{q}} = q, \quad \overline{q + q_1} = \overline{q} + \overline{q_1}, \quad \overline{qq_1} = \overline{q_1}\,\overline{q} \quad \text{e} \quad q\overline{q} = a^2 + b^2 + c^2 + d^2 \qquad (3)$$

delle quali le prime due e l'ultima sono banali, per la terza uguaglianza si veda l'esercizio 9.6.

Possiamo definire la norma $\|q\| = \sqrt{q\bar{q}} = \sqrt{a^2+b^2+c^2+d^2}$. Nell'esercizio 9.7 (si veda anche l'esercizio 10.11) si chiede di provare che

$$\|q \cdot q_1\| = \|q\| \cdot \|q_1\| \text{ per ogni } q, q_1 \in \mathbb{H}.$$

Osserviamo che $\|q\| \geq 0$ e vale $\|q\| = 0$ se e solo se $q = 0$. Se $q \neq 0$ l'ultima uguaglianza $q\bar{q} = \|q\|^2$ in (3) si può interpretare anche nel modo seguente:

$$q \cdot (\|q\|^{-2} \cdot \bar{q}) = (\|q\|^{-2} \cdot \bar{q}) \cdot q = 1.$$

Questo significa che il quaternione

$$q_1 = \|q\|^{-2} \cdot \bar{q} = \frac{a}{\|q\|^2} - \frac{b}{\|q\|^2}i - \frac{c}{\|q\|^2}j - \frac{d}{\|q\|^2}k$$

è l'inverso di q. Pertanto $\mathbb{H}$ è un corpo.

9.4 Sottoanelli

Definizione 9.10. Un sottoinsieme non vuoto B di un anello A si dice *sottoanello* se:

(S1) B è un sottogruppo del gruppo $(A, +)$;
(S2) B è *stabile*, cioè $xy \in B$ per ogni coppia di elementi $x, y \in B$.

Nel caso in cui A sia un anello unitario, si chiede inoltre

(S3) $1_A \in B$.

Dalla (S1) è evidente che $0 \in B$ per ogni sottoanello B di A.

Esempio 9.11. Ci sono sempre i sottoanelli A e $\{0\}$, che chiameremo *banali*. Se A è unitario, allora A è l'unico sottoanello banale di A poiché per (S3) $\{0\}$ non è un sottoanello di A. In certi casi non ci sono sottoanelli non banali: per esempio nell'anello $(\mathbb{Z}_p, +, \cdot)$, con p primo.

Se B è un sottoanello di A e C è un sottoanello di B, allora C è anche un sottoanello di A. Questo resta vero anche quando A è unitario.

Non è difficile verificare che se B e C sono sottoanelli di un anello A, allora $B \cap C$ è un sottoanello di A. Dimostriamo questa proprietà nel caso generale.

Lemma 9.12. *L'intersezione di una famiglia qualsiasi di sottoanelli di un anello A è ancora un sottoanello di A.*

DIMOSTRAZIONE. Sia $\{B_i\}_{i \in I}$ una famiglia di sottoanelli dell'anello A e sia

$$B = \bigcap_{i \in I} B_i.$$

Allora B è un sottogruppo di $(A, +)$ per il lemma 5.30. Per $x, y \in B$ si ha $x, y \in B_i$ per ogni $i \in I$. Quindi (S2) implica $xy \in B_i$ per ogni $i \in I$. Di conseguenza $xy \in B$. Questo dimostra che B è un sottoanello di A. Se A è unitario, allora $1_A \in B_i$ per ogni $i \in I$ e quindi $1_A \in B$. □

Definizione 9.13. Sia A un anello unitario. Il più piccolo sottoanello B non banale di A si dice *sottoanello fondamentale* di A. Non è difficile vedere che B consiste di tutti i multipli del tipo $n \cdot 1_A$, con $n \in \mathbb{Z}$. Se la cardinalità m di B è finita, diciamo che A ha *caratteristica* m, altrimenti si dice che A ha *caratteristica* 0.

Denotiamo con char A la caratteristica di A. In altre parole, la caratteristica di A è $m > 0$ se e solo se

$$\underbrace{1_A + \ldots + 1_A}_{m \text{ volte}} = 0 \quad \text{e} \quad \underbrace{1_A + \ldots + 1_A}_{n \text{ volte}} \neq 0 \text{ per } 1 \leq n < m.$$

Si osservi che char $\mathbb{Z}_m$ = char $M_n(\mathbb{Z}_m) = m$, mentre

$$\text{char } \mathbb{Z} = \text{char } \mathbb{Q} = \text{char } \mathbb{R} = \text{char } \mathbb{C} = \text{char } \mathbb{H} = 0.$$

Siano A un anello e X un sottoinsieme di A. Il sottoanello di A *generato da* X è il più piccolo sottoanello di A contenente X, cioè l'intersezione di tutti i sottoanelli di A che contengono X. Mostriamo un esempio di anello generato da un particolare tipo di insieme.

Esempio 9.14. Sia B un anello commutativo unitario e siano A un sottoanello di B e b un elemento di B. Si dimostra facilmente che il sottoanello di B generato dall'elemento b e dal sottoanello A è l'insieme di tutte le somme della forma

$$a_0 + a_1 b + a_2 b^2 + \ldots + a_n b^n, \quad \text{dove} \quad a_0, a_1, \ldots, a_n \in A.$$

In seguito denoteremo con $A[b]$ il sottoanello descritto nell'esempio 9.14.

9.5 Ideali

Definizione 9.15. Un sottoinsieme I di un anello A che risulta un sottogruppo del gruppo $(A, +)$ si dice

(a) *ideale sinistro* se $ab \in I$ per ogni $a \in A$, $b \in I$.
(b) *ideale destro* se $ba \in I$ per ogni $a \in A$, $b \in I$.
(c) *ideale bilatero* se risulta ideale destro e ideale sinistro.

È chiaro che $\{0\}$ e A sono ideali bilateri di A, chiamati *ideali banali.* Gli ideali di A diversi da A si chiamano *ideali propri* di A.

Un sottoanello B di un anello A potrebbe non essere un ideale (sinistro, destro o bilatero) di A. Più precisamente, se A è unitario, un sottoanello B di A risulta un ideale sinistro o destro se e solo se $B = A$. In altre parole, l'unico ideale (destro o sinistro) di A che risulta essere anche un sottoanello di A è A stesso. Tuttavia un ideale destro o sinistro di un anello non unitario risulta un sottoanello.

Come nel caso dei gruppi, in generale l'unione di due ideali I e J non è un ideale, anzi lo è solo quando un ideale è contenuto nell'altro. Si può estendere questo fatto ad una unione infinita di ideali, nel modo seguente.

Lemma 9.16. *Sia*

$$I_1 \subseteq I_2 \subseteq \dots I_n \subseteq \dots$$

una catena crescente di ideali (destri, sinistri o bilateri) di un anello A. Allora

$$I = \bigcup_{j \in \mathbb{N}} I_j$$

è un ideale (destro, sinistro o bilatero) di A.

DIMOSTRAZIONE. Per il lemma 5.37 I è un gruppo abeliano.

Siano ora $c \in A$ e $a \in I$. Allora $a \in I_k$ per qualche $k \in \mathbb{N}$ e pertanto $ac \in I_k \subseteq I$, se I_k è ideale destro. Analogamente $ca \in I_k$, se I_k è ideale sinistro, oppure valgono entrambe se I_k è un ideale bilatero. □

Nel seguito applicheremo il lemma non solo per successioni (catene) crescenti di ideali $(I_n)_{n \in \mathbb{N}}$, ma anche per catene di ideali più generali $(I_\alpha)_{\alpha \in X}$, dove l'indice α varia in un'insieme totalmente ordinato $(X, \leq)$, cioè per $\alpha \leq \beta$ in X si ha $I_\alpha \subseteq I_\beta$.

Ci occupiamo dell'intersezione di ideali.

Lemma 9.17. *L'intersezione di una famiglia qualsiasi di ideali destri, sinistri o bilateri di un anello A è un ideale rispettivamente destro, sinistro o bilatero di A.*

DIMOSTRAZIONE. Sia $\{J_i\}_{i \in I}$ una famiglia di ideali destri dell'anello A e sia

$$J = \bigcap_{i \in I} J_i.$$

Allora J è un sottogruppo di $(A, +)$ per il lemma 5.30. Per $x \in J$, $a \in A$ si ha $x \in J_i$ per ogni $i \in I$. Quindi (b) della definizione 9.15 implica $xa \in J_i$ per ogni $i \in I$. Di conseguenza $xa \in J$. Questo dimostra che J è un ideale destro di A. Si ragiona analogamente per ideali sinistri o bilateri. □

Definizione 9.18. Se X è un sottoinsieme di A, l'intersezione $(X)_d$ di tutti gli ideali destri di A contenenti X è un ideale destro di A che si dice *ideale destro generato da* X. Analogamente si definisce l'*ideale sinistro* $(X)_s$ *generato da* X e l'*ideale bilatero* (X) *generato da* X.

Chiaramente (X) è *il più piccolo ideale bilatero di A contenente X*. In particolare se $I = (X)$ diremo che X è un sistema di generatori di I oppure che I è generato da X.

Lemma 9.19. *Sia A un anello unitario e sia $X = \{x\}$. Allora l'ideale sinistro generato da X coincide con l'insieme $Ax = \{ax : a \in A\}$.*

DIMOSTRAZIONE. Poiché Ax è un sottogruppo, essendo $ax - bx = (a - b)x$ per ogni $a, b \in A$, basta notare che $bax \in Ax$ per ogni $b, a \in A$. Questo prova che $\{ax : a \in A\}$ è un ideale sinistro. Osserviamo infine che ogni ideale sinistro che contiene x contiene anche Ax. □

Analogamente si può dimostrare che l'ideale destro generato da $X = \{x\}$ coincide con l'insieme $xA = \{xa : a \in A\}$ e che l'ideale bilatero (x) generato da $X = \{x\}$ coincide con l'insieme di tutte le somme del tipo $\sum_{i=1}^{n} a_i x b_i$, al variare a_i, b_i in A, $i = 1, 2, \dots, n$ e $n \in \mathbb{N}$.

Definizione 9.20. Un ideale bilatero I si dice *principale* se $I = (x)$ è generato da un elemento $x \in A$. Un dominio di integrità si dice *dominio a ideali principali* se ogni ideale I di A è principale.

Lemma 9.21. *Sia A anello con unità e sia I ideale sinistro, destro o bilatero di A. Se I contiene un elemento invertibile, allora $I = A$.*

DIMOSTRAZIONE. Sia $u \in I$ un elemento invertibile e supponiamo che I sia un ideale destro. Allora esiste u^{-1} tale che $uu^{-1} = 1 \in I$, poiché I è un ideale destro. Sia $a \in A$, allora $a = 1a \in I$, ancora grazie al fatto che I è un ideale destro. Pertanto $A \subseteq I$, da cui l'uguaglianza $A = I$. Analogamente se I è ideale sinistro o bilatero. □

Dimostriamo ora un utile criterio per verificare se un anello è un campo.

Lemma 9.22. *Sia A un anello commutativo con unità. Allora A è un campo se e solo se A è privo di ideali non banali.*

DIMOSTRAZIONE. Sia A un campo e sia I un ideale non nullo di A. Allora esiste $u \in I$ con $0 \neq u$. Poiché A è un campo, u è invertibile e $I = A$ per il lemma 9.21.

Supponiamo viceversa che A sia privo di ideali non banali. Dobbiamo dimostrare che ogni elemento non nullo $a \in A$ è invertibile. Sia dunque $0 \neq a \in A$; consideriamo l'ideale (a) generato da a: per ipotesi $(a) = A$ e quindi $1 \in (a)$. Esiste pertanto $b \in A$ tale che $1 = ba \in (a)$ per il lemma 9.19. Per l'unicità dell'inverso si ha $b = a^{-1}$. □

Questo criterio si estende al caso non commutativo.

Lemma 9.23. *Per un anello con unità A le seguenti condizioni sono equivalenti:*

(a) A è un corpo;
(b) A è privo di ideali destri non banali;

(c) *A è privo di ideali sinistri non banali.*

DIMOSTRAZIONE. Se A è un corpo, si dimostra come nel lemma 9.22 che ogni ideale destro o sinistro di A è banale, provando così (a) $\Rightarrow$ (b) e (a) $\Rightarrow$ (c).

Supponiamo che A sia privo di ideali destri non banali. Sia $0 \neq a \in A$. Allora aA è un ideale destro non nullo, poiché contiene $a \neq 0$ e quindi $aA = A$. Pertanto esiste $x \in A$ con $ax = 1$. Analogamente, ragionando con x al posto di a si trova un elemento $y \in A$ tale che $xy = 1$. Ora $a = a1 = a(xy) = (ax)y = 1y = y$. Quindi, anche $xa = 1$. Pertanto x è l'inverso di a. Questo dimostra l'implicazione (b) $\Rightarrow$ (a). L'implicazione (c) $\Rightarrow$ (a) si dimostra analogamente. □

Osserviamo che $M_2(\mathbb{R})$ non è un corpo in quanto ha divisori dello zero, per l'esercizio 9.45. Pertanto dal lemma 9.23 deduciamo che $M_2(\mathbb{R})$ ha ideali sinistri e destri non banali, mentre per l'esercizio 9.17 non ha ideali bilateri non banali.

Nell'esempio successivo descriviamo gli ideali sinistri e destri di $M_2(\mathbb{R})$.

Esempio 9.24. Sia $A = M_2(\mathbb{R})$.

(a) Per $(a, b) \in \mathbb{R}^2$ consideriamo l'ideale sinistro $I_{a,b} = A\alpha_{a,b}$, dove

$$\alpha_{a,b} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

Non è difficile dimostrare che ogni matrice non invertibile $\gamma \in A$ si può trasformare, con una sequenza di trasformazioni elementari sulle righe, in una matrice $\alpha_{a,b}$ con opportuni $a, b \in \mathbb{R}$. Ricordiamo che le trasformazioni elementari sulle righe corrispondono nell'anello A alle moltiplicazioni a sinistra tramite opportune matrici di A. Poiché ogni ideale sinistro proprio contiene solo matrici non invertibili, concludiamo che ogni ideale sinistro proprio contiene un ideale sinistro della forma $I_{a,b}$. Ora notiamo che, se $c \in \mathbb{R}$ e $c \neq 0$, allora $I_{a,b} = I_{ac,bc}$. Pertanto la somma $I_{a,b} + I_{a',b'}$ resta un ideale sinistro proprio se e solo se i vettori (a, b) e (a', b') di $\mathbb{R}^2$ sono linearmente dipendenti. In tal caso $I_{a,b} = I_{a',b'}$. Di conseguenza, ogni ideale sinistro proprio di A coincide o con $I_{0,1}$ oppure con uno degli ideali sinistri $I_{1,r}$, $r \in \mathbb{R}$.

(b) Analogamente si dimostra che ogni ideale destro proprio ha la forma

$$J_{a,b} = \beta_{a,b}A, \quad \text{dove} \quad \beta_{a,b} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}.$$

Inoltre $J_{a,b} = J_{ac,bc}$ se $c \in \mathbb{R}$ e $c \neq 0$. Quindi ogni ideale destro proprio di A coincide o con $J_{0,1}$ oppure con uno degli ideali destri $J_{1,r}$, $r \in \mathbb{R}$.

Similmente si trovano gli ideali sinistri e destri dell'anello $M_2(K)$, dove K è un campo arbitrario.

9.6 L'anello quoziente

Se I è un ideale bilatero di un anello A, introduciamo in A una relazione binaria ponendo per $x, y \in A$

$$x \sim y \quad \text{se} \quad x - y \in I.$$

Abbiamo dimostrato nel lemma 5.44 che $\sim$ è una relazione di equivalenza le cui classi di equivalenza $[x]_\sim$ sono le classi laterali $x + I = \{x + i : i \in I\}$.

Sia A un anello e sia I un ideale bilatero di A. Sappiamo dal teorema 6.1 che la relazione di equivalenza appena introdotta è compatibile con l'operazione del gruppo $(A, +)$. Proviamo che $\sim$ è compatibile anche con l'operazione moltiplicazione dell'anello A nel senso che

$$\text{se } x \sim x_1 \text{ e } y \sim y_1, \text{ allora } xy \sim x_1y_1. \tag{4}$$

Infatti per la definizione di $\sim$ si ha $x_1 = x + h$ e $y_1 = y + h'$ per opportuni $h, h' \in I$. Allora

$$x_1y_1 = (x + h)(y + h') = xy + hy + xh' + hh'.$$

Si ha $hy, xh', hh' \in I$, perché I è ideale bilatero di A. Pertanto $xy \sim x_1y_1$.

Teorema 9.25. *Nel gruppo quoziente $(A/I, +)$ si introduce un'operazione binaria $\cdot$ ponendo $(x + I) \cdot (y + I) = xy + I$. Con il prodotto così definito $(A/I, +, \cdot)$ risulta un anello, detto* anello quoziente. *Se A è unitario, allora anche A/I è unitario. Se A è commutativo, allora anche A/I è commutativo.*

DIMOSTRAZIONE. Si osservi che per (4), tale operazione è ben definita. Verifichiamo la legge associativa:

$$((x + I) \cdot (y + I)) \cdot (z + I) = (xy + I) \cdot (z + I) = ((xy)z) + I =$$

$$= (x(yz)) + I = (x + I) \cdot (yz + I) = (x + I) \cdot ((y + I) \cdot (z + I)).$$

Nel caso in cui A sia unitario, la classe dell'elemento 1 risulta essere l'unità di $(A/I, \cdot)$:

$$(1 + I) \cdot (x + I) = (1 \cdot x) + I = x + I \;\text{ e }\; (x + I) \cdot (1 + I) = (x \cdot 1) + I = x + I$$

per ogni $x \in A$.

Analogamente, se A è commutativo

$$(x + I)(y + I) = xy + I = yx + I = (y + I)(x + I),$$

per ogni $x, y \in A$. □

Esempio 9.26. Sia $m > 1$ un intero. Allora $m\mathbb{Z} = (m)$ è un ideale di $\mathbb{Z}$. La relazione di equivalenza associata all'ideale $m\mathbb{Z}$ è definita da $x \sim y$ se e solo se $y - x \in m\mathbb{Z}$, ovvero $x \equiv_m y$. In altre parole, in questo caso troviamo la congruenza modulo m introdotta nel paragrafo 3.5. Quindi le classi laterali $x + m\mathbb{Z}$ coincidono con le classi $[x]_m$ dei resti modulo m. Perciò l'anello quoziente $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ in questo caso coincide con l'anello $(\mathbb{Z}_m, +, \cdot)$ introdotto in precedenza.

9.7 Ideali primi e ideali massimali in anelli commutativi

Definizione 9.27. Un ideale (sinistro, destro o bilatero) proprio I di un anello A si dice *massimale* se per ogni ideale (sinistro, destro o bilatero rispettivamente) tale che $I \subseteq J \subseteq A$ si ha $I = J$ oppure $J = A$.

Definizione 9.28. Un ideale proprio I di un anello commutativo A si dice *primo* se per ogni coppia di elementi $x, y \in A$, $xy \in I$ implica $x \in I$ o $y \in I$.

Teorema 9.29. *Sia A un anello commutativo unitario. Allora un ideale I di A è primo se e solo se il quoziente A/I è un dominio.*

DIMOSTRAZIONE. Supponiamo che I sia primo. Allora per

$$\overline{x} = x + I, \quad \overline{y} = y + I \in A/I \quad \text{si ha } \overline{xy} = \overline{0} \quad \text{se} \quad xy \in I.$$

In tal caso $x \in I$ o $y \in I$, cioè $\overline{x} = \overline{0}$ o $\overline{y} = \overline{0}$. Quindi A/I non ha divisori dello zero.

Supponiamo ora che A/I non abbia divisori dello zero. Siano $x, y \in A$ con $xy \in I$. Allora per $\overline{x} = x + I, \overline{y} = y + I \in A/I$ si ha $\overline{xy} = \overline{0}$ in A/I. Essendo A/I un dominio, concludiamo che $\overline{x} = \overline{0}$ o $\overline{y} = \overline{0}$, cioè $x \in I$ o $y \in I$. □

Analogamente, per verificare se un ideale I di un anello commutativo A è massimale è sufficiente controllare l'anello quoziente.

Teorema 9.30. *Sia A un anello commutativo unitario. Allora I è massimale se e solo se il quoziente A/I è un campo.*

DIMOSTRAZIONE. Supponiamo che I sia massimale. Allora per ogni elemento non nullo $a + I \in A/I$ l'ideale $J = I + (a)$ di A contiene propriamente I, quindi $J = A$. Pertanto esistono $x \in A$ e $i \in I$ con $1 = i + ax$. In altre parole, $1 - ax = i \in I$, quindi $ax + I = 1 + I$. Dunque $(a + I)(x + I) = 1 + I$, pertanto $a + I$ è invertibile in A/I. Questo dimostra che A/I è un campo.

Supponiamo ora che A/I sia un campo. Sia J un ideale di A contenente I propriamente. Allora esiste $a \in J$ con $a \notin I$. Allora $a + I$ è un elemento non nullo del campo A/I. Quindi esiste $x + I \in A/I$ con $(a + I)(x + I) = 1 + I$. Dunque $ax + I = 1 + I$ e di conseguenza $1 - ax = i \in I$. Ora $1 = ax + i \in J$. Questo dimostra che $J = A$. □

Corollario 9.31. *Sia A un anello commutativo unitario, allora ogni ideale massimale è un ideale primo.*

DIMOSTRAZIONE. Sia I un ideale massimale di A. Allora per il teorema 9.30, il quoziente A/I è un campo e di conseguenza anche un dominio, quindi per il teorema 9.29 l'ideale I è primo. □

Nell'esercizio 9.47 si dimostra che in $\mathbb{Z}$ esistono infiniti ideali massimali. Per un anello che ammette un unico ideale massimale, si introduce un nome specifico.

Definizione 9.32. Sia A un anello commutativo con identità 1 e sia I un ideale proprio di A tale che, per ogni ideale proprio J di A, si ha $J \subseteq I$. Allora A si dice un *anello locale*.

Vari esempi di anelli locali e loro proprietà si possono trovare negli esercizi 9.48, 9.49, 9.50 e 10.23.

Dimostriamo ora un teorema, noto come *teorema di Krull*, che garantisce che ogni ideale proprio di un anello commutativo unitario è contenuto in un ideale massimale.

Teorema 9.33. (Teorema di Krull) *Sia A un anello commutativo unitario e sia I un ideale proprio di A. Allora esiste un ideale massimale M di A contenente I.*

DIMOSTRAZIONE. Consideriamo la famiglia $\mathcal{I}$ degli ideali propri di A che contengono I. Visto che $I \in \mathcal{I}$, abbiamo $\mathcal{I} \neq \emptyset$. Ordiniamo $\mathcal{I}$ con l'inclusione $\subseteq$. Sia $\mathcal{I}_1$ un sottoinsieme totalmente ordinato di $\mathcal{I}$. Allora $J = \bigcup\{L : L \in \mathcal{I}_1\}$ è un ideale di A contenente I per il lemma 9.16 e il successivo commento. Verifichiamo che J è un ideale proprio di A. Infatti $1 \notin L$ per ogni $L \in \mathcal{I}_1$, essendo L proprio. Quindi $1 \notin J$. Pertanto $J \in \mathcal{I}$ e ovviamente $L \subseteq J$ per ogni $L \in \mathcal{I}_1$. Quindi J è un maggiorante di $\mathcal{I}_1$. Abbiamo così dimostrato che l'insieme ordinato $\mathcal{I}$ è induttivo. Applicando il lemma di Zorn deduciamo che $\mathcal{I}$ ha un elemento massimale M. Chiaramente M è un ideale massimale e M contiene I. □

Il teorema di Krull non vale in anelli commutativi senza unità, come dimostra il seguente esempio.

Esempio 9.34. Sia $(A, +)$ un gruppo abeliano. Possiamo renderlo un anello con la moltiplicazione triviale $ab = 0$ per ogni $a, b \in A$. Allora gli ideali di A sono precisamente i sottogruppi di A. In particolare gli ideali massimali dell'anello A coincidono con i sottogruppi massimali del gruppo A. Quindi per trovare un esempio di anello commutativo senza ideali massimali basta prendere il gruppo abeliano $\mathbb{Z}_{p^\infty}$ descritto nell'esempio 7.21.

9.8 Esercizi su anelli e ideali

Esercizio 9.1 Trovare i divisori dello zero e gli elementi nilpotenti di $\mathbb{Z}_{12}$, $\mathbb{Z}_{15}$ e $\mathbb{Z}_{16}$.

Esercizio 9.2 Provare che un anello A è privo di divisori destri dello zero se e solo se è privo di divisori sinistri dello zero.

Esercizio 9.3 Dimostrare che, se A è un anello, allora l'insieme $M_n(A)$ delle matrici quadrate $n \times n$ a coefficienti in A, con l'usuale somma e prodotto righe per colonne, risulta essere un anello.

Esercizio 9.4 Sia A un anello e sia S un insieme non vuoto. Sia

$$A^S = \{f : S \to A,\ f \text{ funzione}\}.$$

Si definiscano

$$(f+g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x)g(x) \quad \forall\, x \in S, \quad f, g \in A^S.$$

Si dimostri che $(A^S, +, \cdot)$ è un anello, A^S è commutativo se e solo se A è commutativo e A^S è unitario se e solo se A è unitario.

Esercizio 9.5 Sia A un anello e siano $a, b \in A$ due elementi che commutano. Dimostrare che vale:

(a) la formula del binomio per $(a+b)^n$;
(b) la formula $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$;
(c) la formula $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots + (-1)^{n-1}b^{n-1})$ se n è dispari.

Esercizio 9.6 Dimostrare che vale l'uguaglianza $\overline{q_1 q_2} = \overline{q}_2 \overline{q}_1$ per ogni coppia $q_1, q_2 \in \mathbb{H}$.

Esercizio 9.7 Dimostrare che vale l'uguaglianza $\|q_1 q_2\| = \|q_1\| \|q_2\|$ per ogni coppia $q_1, q_2 \in \mathbb{H}$.

Esercizio 9.8 Sia $q_0 \in \mathbb{H}$ e $B(q_0) = \{q \in \mathbb{H} : qq_0 = q_0 q\}$. Dimostrare che:

(a) $B(q_0)$ è un sottoanello di $\mathbb{H}$ che risulta un corpo;
(b) $B(q_0)$ è un sottospazio vettoriale di $\mathbb{H}$ contenente $\mathbb{R}$;
(c) $B(q_0) = \mathbb{H}$ se e solo se $q_0 \in \mathbb{R}$, più precisamente $B(q_0) = \mathbb{R} + \mathbb{R}q_0$ se e solo se $q_0 \notin \mathbb{R}$.
(d) se $q \in B(q_0)$, allora anche $\overline{q} \in B(q_0)$,
(e) se $q \in B(q_0)$, allora $\overline{q} \in B(\overline{q_0})$, ovvero $B(\overline{q_0}) = B(q_0)$.

Esercizio 9.9 Per un quaternione $q = a + bi + cj + dk \in \mathbb{H}$ denotiamo con $Re(q)$ il numero reale a e la chiamiamo *parte reale* di q. Provare che se $0 \neq q^2 \in \mathbb{R}$ e $q \notin \mathbb{R}$, allora $Re(q) = 0$ e $q^2 < 0$.

Esercizio 9.10 Dimostrare che per un elemento q del gruppo $(\mathbb{H}^*, \cdot)$ valgono le seguenti proprietà:

(a) se $Re(q) = 0$, allora $q^2 = -\|q\|^2$;
(b) se q è periodico, allora $\|q\| = 1$;
(c) se $q \neq \pm 1$, allora q ha periodo 4 se e solo se $Re(q) = 0$ e $\|q\| = 1$.

Esercizio 9.11 Sia A il sottoanello di $\mathbb{H}$ generato da i e j. Trovare il numero delle soluzioni dell'equazioni $q^2 + 9 = 0$, $q^2 + 17 = 0$, $q^2 + 29 = 0$ e $q^2 + 41 = 0$ in A.

Esercizio 9.12 * Dimostrare che per $q_1, q_2 \in \mathbb{H}$, non reali, le seguenti condizioni sono equivalenti:

(a) $\|q_1\| = \|q_2\|$ e $Re(q_1) = Re(q_2)$;

(b) esiste $0 \neq q_0 \in \mathbb{H}$ tale che $q_2 = q_0^{-1} q_1 q_0$.

Esercizio 9.13 Sia S l'insieme dei quaternioni di norma 1. Dimostrare che:

(a) S è un sottogruppo di $(\mathbb{H}^*, \cdot)$;
(b) $Z(S) = \{\pm 1\}$;
(c) * il gruppo quoziente $S/Z(S)$ è semplice.

Esercizio 9.14 Sia A un anello. Descrivere:

(a) il sottoanello di A generato da un dato elemento $a \in A$;
(b) il sottoanello di A generato da due elementi $a, b \in A$ che commutano.

Si consideri il caso di un anello unitario A.

Esercizio 9.15 Siano I_1 e I_2 due ideali sinistri (rispettivamente destri) dell'anello A. Provare che $I_1 + I_2 = \{x + y : x \in I_1, y \in I_2\}$ è un ideale sinistro (rispettivamente destro) dell'anello A. Se I_1 e I_2 sono ideali bilateri, allora anche $I_1 + I_2$ è un ideale bilatero.

Esercizio 9.16 Sia I un ideale bilatero di un anello A e sia B un sottoanello di A. Provare che $I + B = \{x + y : x \in I, y \in B\}$ è un sottoanello di A.

Esercizio 9.17 Dimostrare che ogni ideale bilatero dell'anello $M_2(\mathbb{R})$ è banale.

Esercizio 9.18 Sia $n \in \mathbb{N}$. Verificare che l'insieme $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ è un ideale di $\mathbb{Z}$ e provare che ogni ideale di $\mathbb{Z}$ ha questa forma.

Esercizio 9.19 Sul gruppo abeliano $A = (\mathbb{R}, +) \times (\mathbb{R}, +)$ si consideri la moltiplicazione definita da $(x, y) \cdot (x', y') = (xx' + yy', xy' + x'y)$.

(a) Dimostrare che in questo modo $(A, +, \cdot)$ risulta un anello unitario da cui $\mathbb{R} \times \{0\}$ è un sottoanello.
(b) Caratterizzare gli elementi invertibili ed i divisori dello zero di A.
(c) Dire se esistono elementi che non sono né divisori dello zero né invertibili.
(d) Trovare gli ideali massimali di A.

Esercizio 9.20* Sia R un anello commutativo unitario e sia $G = \{g_1, g_2, \ldots, g_n\}$ un gruppo finito. Sull'insieme $R[G]$ di tutte le combinazioni lineari del tipo

$$\sum_{i=1}^{n} r_i g_i, \qquad r_i \in R,$$

si considerino le operazioni + e $\cdot$ definite come segue:

$$\left(\sum_{i=1}^{n} r_i g_i\right) + \left(\sum_{i=1}^{n} r'_i g_i\right) = \sum_{i=1}^{n} (r_i + r'_i) g_i \quad \text{e}$$

$$\left(\sum_{i=1}^{n} r_i g_i\right) \cdot \left(\sum_{i=1}^{n} r'_i g_i\right) = \sum_{i=1}^{n} s_i g_i, \text{ dove } s_i = \sum_{g_j g_k = g_i} r_j r'_k.$$

Si dimostri che $R[G]$ munito con le operazioni + e $\cdot$ risulta un anello, detto *anello gruppale*.

(a) Provare che $R[G]$ è anello unitario.
(b) Provare che se G non è banale, $R[G]$ ha divisori dello zero.
(c) Sia G un gruppo con due elementi. Dimostrare che $\mathbb{R}[G]$ è isomorfo all'anello definito nell'esercizio 9.19. Sia g_2 il generatore di G. Provare che $I_1 = (g_2 + 1)$ e $I_2 = (g_2 - 1)$ sono gli unici ideali di $\mathbb{R}[G]$ e $\mathbb{R}[G]/I_1 \cong \mathbb{R}[G]/I_2 \cong \mathbb{R}$.
(d) Sia $(G, \cdot)$ un gruppo ciclico di ordine quattro e generatore b. Si considerino i tre ideali $I_0 = (b^2 + 1)$, $I_1 = (b + 1)$ e $I_2 = (b - 1)$ dell'anello $\mathbb{R}[G]$. Dimostrare che $\mathbb{R}[G]/I_0 \cong \mathbb{C}$ e $\mathbb{R}[G]/I_1 \cong \mathbb{R}[G]/I_2 \cong \mathbb{R}$ e dedurre che I_0, I_1 e I_2 sono ideali massimali.
(e) Sia $A = \mathbb{R}[Q_8]$, con Q_8 il gruppo dei quaternioni definito nel lemma 5.81. Dimostrare che per $i \in Q_8$ l'elemento $i^2 + 1$ di A è divisore dello zero e commuta con ogni elemento di A. Sia $I = (i^2 + 1)$ l'ideale principale generato da $i^2 + 1$, si dimostri che $A/I \cong \mathbb{H}$, il corpo dei quaternioni.

Esercizio 9.21 Sia A un anello con identità 1. Si deduca dal lemma 9.12 che l'insieme $\mathcal{L}(A)$ dei sottoanelli di A ordinato per inclusione è un reticolo limitato avente A come elemento massimo e il sottoanello fondamentale di A come minimo elemento.

Esercizio 9.22 Studiare gli elementi nilpotenti dell'anello $\mathbb{Z}/n\mathbb{Z}$.

(a) Siano $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, $p_1, \dots, p_t$ primi distinti e $\alpha_i \geq 1$ per ogni $i \leq t$. Dimostrare che $a + n\mathbb{Z}$ è nilpotente se e solo se $p_1 \dots p_t$ divide a.
(b) Provare che l'anello $\mathbb{Z}/n\mathbb{Z}$ è privo di elementi nilpotenti non nulli se e solo se $n = p_1 \dots p_t$, p_i primi distinti.
(c) Determinare gli elementi nilpotenti di ciascuno degli anelli $\mathbb{Z}_{10}, \mathbb{Z}_{18}, \mathbb{Z}_{20}, \mathbb{Z}_{21}, \mathbb{Z}_{24}$.

Esercizio 9.23 Sia A un anello commutativo unitario e a un elemento di A.

(a) Dimostrare che se a è nilpotente, allora $a + 1$ è invertibile.
(b) Dimostrare che se a è nilpotente e u è invertibile, allora $a + u$ è invertibile.
(c) Dimostrare che l'insieme $N(A)$ di tutti gli elementi nilpotenti di A è un ideale.
(d) Calcolare $N(\mathbb{Z}_{36})$. Calcolare $N(\mathbb{Z}_{p^n})$, dove p è un primo e $n \in \mathbb{N}$.

Esercizio 9.24 * Sia A un anello commutativo unitario. Dimostrare che l'ideale $N(A)$ descritto nell'esercizio 9.23 coincide con l'intersezione di tutti gli ideali primi di A.

Esercizio 9.25 Sia A un anello commutativo unitario finito. Si dimostri che:

(a) ogni ideale primo di A è massimale;
(b) esiste un $k \in \mathbb{N}$ tale che $a^k = 0$ per tutti gli elementi nilpotenti di A.

Esercizio 9.26 Siano A un anello commutativo e $a, b \in A$. Supponiamo che esistano interi positivi m, n coprimi tali che $a^m = b^m$ e $a^n = b^n$. Quando si può concludere che $a = b$?

Esercizio 9.27 Sia A un anello commutativo unitario e $X = \{x, y\}$. Si provi che l'ideale sinistro generato da X coincide con l'insieme delle somme $\{ax + by : a \in A, b \in A\}$, cioè $Ax + Ay$.

Esercizio 9.28 Sia A un anello unitario. Si dimostri che l'ideale bilatero (a) coincide con l'insieme di tutte le somme del tipo $x_1ay_1 + \ldots + x_nay_n$, dove $x_1, y_1, \ldots, x_n, y_n \in A$.

Esercizio 9.29 Sia A un anello commutativo e H, K ideali di A. Si definisce l'insieme:

$$HK = \{h_1k_1 + \cdots + h_nk_n : n \in \mathbb{N},\ h_i \in H, k_i \in K, i = 1, \ldots, n\}.$$

(a) Provare che HK è un ideale contenuto nell'ideale $H \cap K$.
(b) Provare che se $A = \mathbb{Z}$, $H = 4\mathbb{Z}$, $K = 6\mathbb{Z}$, allora $HK \neq H \cap K$.
(c) Provare che se A è un anello unitario e $H + K = A$, allora $HK = H \cap K$.
(d) Provare che l'affermazione in (c) non è vera se A non è un anello unitario.

Esercizio 9.30 Sia A un anello commutativo unitario e H, K ideali di A. Sia HK l'insieme definito nell'esercizio 9.29.

(a) Per $n \in \mathbb{N}_+$ definire K^n per induzione: $K^1 = K$, $K^2 = KK$, $K^n = K^{n-1}K$, se $n > 1$. Dimostrare che se K è un ideale massimale, allora l'unico ideale massimale che contiene K^n per $n \in \mathbb{N}_+$ è K.
(b) Dimostrare che se K è un ideale massimale, allora il quoziente A/K^n è un anello locale per ogni $n \in \mathbb{N}_+$.
(c) Se $H + K = A$, provare che anche $H^n + K^n = A$ per ogni $n \in \mathbb{N}_+$.
(d) Se J è un ideale di A tale che $H + J = K + J = A$, provare che anche $(H \cap K) + J = A$.
(e) Siano $I_0, I_1, \ldots, I_n$ $(n \geq 2)$ ideali di A tali che $I_0 + I_k = A$ per $k = 1, 2, \ldots, n$. Provare che anche $I_0 + \bigcap_{k=1}^n I_k = A$.
(f) Siano $I_1, \ldots, I_n$ $(n \geq 2)$ ideali di A tali che $I_j + I_k = A$ per $1 \leq j < k \leq n$. Provare che $\bigcap_{k=1}^n I_k = I_1I_2 \ldots I_n$.

Esercizio 9.31 Sia A un anello commutativo unitario finito e siano $M_1, M_2, \ldots, M_s$ tutti i suoi ideali massimali. Allora esiste $k \in \mathbb{N}$ tale che

$$M_1^k \cap M_2^k \cap \ldots \cap M_s^k = (M_1M_2 \ldots M_s)^k = \{0\}.$$

Esercizio 9.32 * Determinare tutti i sottoanelli B di $\mathbb{Q}$.

Esercizio 9.33 (a) Se B_1 e B_2 sono sottoanelli di $\mathbb{Q}$ allora anche $B_1 + B_2$ è un sottoanello di $\mathbb{Q}$.

(b) Trovare due sottoanelli B_1 e B_2 di $\mathbb{R}$ tali che $B_1 + B_2$ non è un sottoanello di $\mathbb{R}$.

Esercizio 9.34 Siano A un anello commutativo e H, K ideali di A. Provare che:

(a) $(H : K) = \{a \in A : ak \in H$ per tutti i $k \in K\}$ è ideale di A;
(b) $H \subset (H : K)$;
(c) $(H : K)K \subset H$;
(d) $(H :\ H + K) = (H : K)$;
(e) se $m, n \in \mathbb{N}$, $d = (m, n)$ e $q = m/d$, allora $(m\mathbb{Z} : n\mathbb{Z}) = q\mathbb{Z}$.

Esercizio 9.35 Sia A un anello privo di divisori dello zero. Dimostrare che, se per qualche elemento $a \in A$ vale $ax = x$ e $ya = y$ per opportuni elementi non nulli $x, y \in A$, allora a è l'unità dell'anello A.

Esercizio 9.36 Sia A un anello commutativo unitario e siano I e J ideali di A. Provare che:

(a) se I e J sono due ideali massimali distinti, allora $IJ = I \cap J$;
(b) se $I = (a)$ e $J = (b)$ sono principali, allora $IJ = (ab)$;
(c) mostrare con un esempio che in generale $IJ \neq I \cap J$;
(d) se I e J sono finitamente generati, allora anche IJ è finitamente generato;
(e) confrontare IJ e $I \cap J$ in $A = \mathbb{Z}$ e $B = \mathbb{R}^S$, dove S è un insieme non vuoto.

Esercizio 9.37 Sia

$$A = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}_3 \right\}.$$

Provare che A è sottocampo di $M_2(\mathbb{Z}_3)$. Provare inoltre che il gruppo $(A^*, \cdot)$ è ciclico, determinare l'ordine di A e un suo generatore.

Esercizio 9.38 Sia

$$A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$

Provare che A è un sottocampo di $M_2(\mathbb{R})$ isomorfo a $\mathbb{C}$.

Esercizio 9.39 Sia A un anello, I ideale di A,

$$U_1 = \{x \in U(A) : x \equiv_I 1\}.$$

Provare che U_1 è sottogruppo normale di $U(A)$.

Esercizio 9.40 Sia $A = \{\frac{m}{n} \in \mathbb{Q} : n \text{ dispari}\} \subseteq \mathbb{Q}$.

(a) Provare che A è sottoanello di $\mathbb{Q}$.
(b) Determinare gli elementi invertibili di A.
(c) Dimostrare che l'insieme I degli elementi non invertibili di A è l'ideale $I = (2)$.
(d) Mostrare che se J è ideale proprio di A, allora $J \subseteq I$.
(e) Determinare tutti gli ideali non banali di A.

Esercizio 9.41 Sia $A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$.

(a) Provare che A è un anello commutativo, ma non è un dominio;
(b) determinare l'insieme $N(A)$ degli elementi nilpotenti di A;
(c) mostrare che ogni ideale proprio di A è contenuto in $N(A)$;
(e) determinare tutti gli ideali di A.

Esercizio 9.42 Nell'anello $M_2(\mathbb{Z}_8)$, sia $A = \left\{ \begin{pmatrix} a & 5b \\ 4b & a \end{pmatrix} : a, b \in \mathbb{Z}_8 \right\}$.

(a) Verificare che A è sottoanello di $M_2(\mathbb{Z}_8)$, dire se A è ideale;

(b) provare che A è anello commutativo unitario;
(c) dire se A è dominio di integrità.

Esercizio 9.43 Fissato un numero intero m, si consideri l'insieme

$$R_m = \left\{ \begin{pmatrix} a & b \\ mb & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

Provare che:

(a) R_m è sottoanello di $M_2(\mathbb{Q})$;
(b) R_m è anello commutativo unitario;
(c) se m non è quadrato di un numero razionale, allora R_m è un campo. Se m è quadrato di un numero razionale, allora in R_m ci sono divisori dello zero.

Esercizio 9.44 Sia $R_m = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Z}_m \right\}$.

(a) Provare che R_m è sottoanello di $M_2(\mathbb{Z}_m)$.
(b) Sia $m = 7$. Verificare che $I = \left\{ \begin{pmatrix} 3k & k \\ 2k & 3k \end{pmatrix} : k \in \mathbb{Z}_7 \right\}$ è ideale. R_7 è campo?
(c) Dire se R_5 è un campo.

Esercizio 9.45 Trovare divisori destri e sinistri dello zero nell'anello $M_2(\mathbb{R})$.

Esercizio 9.46 Sia A un anello locale con un unico ideale massimale I. Dimostrare che le seguenti condizioni sono equivalenti:

(a) $x \in I$;
(b) x non è invertibile, cioè non esiste $y \in A$ con $xy = 1$;
(c) per ogni $y \in A$, $1 + xy$ è invertibile.

Esercizio 9.47 Si dimostri che gli ideali massimali di $\mathbb{Z}$ sono gli ideali $m\mathbb{Z}$, con m primo.

Esercizio 9.48 Per quali valori di m l'anello $\mathbb{Z}_m$ risulta locale?

Esercizio 9.49 Sia p un primo e $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} : p \text{ non divide } n\}$.

(a) Provare che $\mathbb{Z}_{(p)}$ è sottoanello di $\mathbb{Q}$.
(b) Determinare gli elementi invertibili di $\mathbb{Z}_{(p)}$.
(c) Determinare gli ideali di $\mathbb{Z}_{(p)}$.
(d) Determinare gli ideali primi e gli ideali massimali di $\mathbb{Z}_{(p)}$.
(e) Provare che $\mathbb{Z}_{(p)}$ è un anello locale.

Esercizio 9.50 Dimostrare che:

(a) ogni campo è un anello locale senza elementi nilpotenti non nulli;
(b) se l'anello $\mathbb{Z}_m$ risulta locale e non ha elementi nilpotenti non nulli, allora $\mathbb{Z}_m$ è un campo;

(c) dare un esempio di un anello locale senza elementi nilpotenti non nulli che non sia un campo.

Esercizio 9.51 Un anello commutativo A si dice *regolare* se per ogni elemento x di A esiste un altro elemento $y \in A$ con $x = yx^2$. Dimostrare che:

(a) ogni campo è un anello regolare e se A è un dominio regolare, allora A è un campo;
(b) l'anello quoziente di un anello regolare è regolare;
(c) in un anello regolare ogni ideale primo di A è massimale;
(d) in un anello regolare ogni ideale principale è generato da un idempotente;
(e) per ogni insieme non vuoto S gli anelli $\mathbb{Q}^S$ e $\mathbb{R}^S$ sono regolari; più in generale, K^S è regolare per ogni campo K.

Omomorfismi e prodotti diretti di anelli

Questo capitolo è dedicato al concetto di omomorfismo di anello ed altri ad esso associati: prodotto diretto di anelli e anello dei quozienti. Nei primi due paragrafi introduciamo l'omomorfismo di anelli e proviamo i tre teoremi di omomorfismo per gli anelli, in analogia con il caso dei gruppi. Nel terzo paragrafo si considera l'immersione di un anello in un altro anello con proprietà migliori: per esempio l'immersione in anelli unitari, oppure l'immersione di un dominio nel suo campo dei quozienti. Nel quarto paragrafo studiamo i prodotti diretti di anelli, mentre il quinto è dedicato ad altre strutture algebriche che sono associate o simili agli anelli, quali i reticoli e le algebra di Boole. Esso può essere tralasciato durante una prima lettura.

10.1 Omomorfismi e nuclei

Un omomorfismo tra due anelli A e B è un'applicazione da A in B che risulta un omomorfismo tra i gruppi abeliani $(A, +)$ e $(B, +)$ e *rispetta* la struttura di anello. Più precisamente:

Definizione 10.1. Se A e B sono anelli, un *omomorfismo di anelli* di A in B è un'applicazione $\varphi\colon A \to B$ tale che per ogni $a, b \in A$ risulti

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{e} \quad \varphi(ab) = \varphi(a)\varphi(b).$$

Se φ è anche biettiva, φ si dice un *isomorfismo*. Se A e B sono anelli unitari, φ si dice un *omomorfismo di anelli unitari* se $\varphi(1_A) = 1_B$.

Un omomorfismo di anelli di A in sé stesso si dice un *endomorfismo di anelli*, e un isomorfismo si dice un *automorfismo di anelli.*

Nel seguito ometteremo spesso la specifica *di anelli* quando è abbastanza chiaro dal contesto che si tratta di un omomorfismo di anelli.

Si verifica facilmente che la composizione di omomorfismi è ancora un omomorfismo, si veda l'esercizio 10.2.

Sia $\varphi\colon A \to B$ un omomorfismo di anelli. L'insieme $\{a \in A | \varphi(a) = 0_B\}$ si dice *nucleo* di φ e si indica con $\ker \varphi$.

Proposizione 10.2. *Sia* $\varphi\colon A \to B$ *un omomorfismo di anelli. Allora*

(a) $\varphi(0_A) = 0_B$*;*
(b) $\ker\varphi$ *è un ideale bilatero di* A*.*

DIMOSTRAZIONE. Dalla proposizione 6.8 risulta che $\ker f$ è un sottogruppo. Verifichiamo che $\ker f$ è un ideale bilatero. Siano $x, y \in A$ e $a \in \ker f$. Allora

$$\varphi(xay) = \varphi(x)\varphi(a)\varphi(y) = \varphi(x)0\varphi(y) = 0,$$

quindi $xay \in \ker f$. □

Ogni ideale bilatero risulta essere il nucleo di qualche omomorfismo. Siano A un anello e I un ideale bilatero di A. Si consideri l'applicazione canonica

$$\pi : A \to A/I \quad \text{definita da } \pi(x) = x + I.$$

È facile vedere che π è un omomorfismo. Inoltre π è suriettivo e $\ker\pi = I$. Chiameremo $\pi : A \to A/I$ *omomorfismo canonico.*

Lemma 10.3. *Sia* $f : A \to A_1$ *un omomorfismo. Allora:*

(a) $f(x) = f(y)$ *per* $x, y \in A$ *se e solo se* $y \in x + \ker f$*;*
(b) $f^{-1}(f(x)) = x + \ker f$ *per ogni* $x \in A$*;*
(c) φ *è iniettivo se e solo se* $\ker\varphi = \{0\}$.

DIMOSTRAZIONE. È noto dal caso dei gruppi. □

10.2 Teoremi di omomorfismo per anelli

Lo scopo del seguente teorema è di presentare un omomorfismo arbitrario f tra due anelli A, A_1 come composizione di due omomorfismi più semplici, dei quali il primo è l'omomorfismo canonico $\pi : A \to A/I$, mentre il secondo è iniettivo.

Teorema 10.4. (Primo teorema di omomorfismo per anelli) *Sia* $f : A \to A_1$ *un omomorfismo. Allora:*

(a) esiste un omomorfismo iniettivo $\tilde{f} : A/\ker f \to A_1$ *tale che* $\tilde{f} \circ \pi = f$*;*
(b) $\tilde{f}$ *è un isomorfismo se e solo se* f *è suriettivo.*

DIMOSTRAZIONE. Dal teorema di omomorfismo 6.12 per i gruppi sappiamo che esiste un'applicazione $\tilde{f}$ definita da

$$\tilde{f}(x + \ker f) = f(x)$$

per ogni $x \in A$, tale che $\tilde{f} \circ \pi = f$. Inoltre $\tilde{f}$ è un omomorfismo iniettivo di gruppi. Per vedere che $\tilde{f}$ è anche un omomorfismo di anelli notiamo che

$$\tilde{f}((x + \ker f) \cdot (y + \ker f)) = \tilde{f}(xy + \ker f) = f(xy) =$$

$$= f(x)f(y) = \bar{f}(x + \ker f) \cdot \bar{f}(y + \ker f).$$

Questo conclude la dimostrazione del punto (a). Il punto (b) segue immediatamente dalle proprietà di $\bar{f}$ garantite dal teorema di omomorfismo per i gruppi. □

Corollario 10.5. *Sia $f : A \to A_1$ un omomorfismo. Allora*

$$A/\ker f \cong f(A).$$

Teorema 10.6. (Teorema di corrispondenza) *Siano A_1, A_2 anelli e $f : A_1 \to A_2$ un omomorfismo.*

(a) Se H è sottoanello di A_1 e C è sottoanello di A_2, allora $f(H)$ è sottoanello di A_2 e $f^{-1}(C)$ è sottoanello di A_1. Questo vale anche quando A_1 e A_2 sono anelli unitari e f è un omomorfismo di anelli unitari.

(b) se I è ideale (destro, sinistro, bilatero) di A_2, allora $f^{-1}(I)$ è ideale (rispettivamente destro, sinistro, bilatero) di A_1 e contiene il nucleo di f;

(c) se J è ideale (destro, sinistro, bilatero) di A_1, allora $f(J)$ è ideale (rispettivamente destro, sinistro, bilatero) di $f(A_1)$.

(d) $f^{-1}(f(B)) = \ker f + B$ per ogni sottoanello o ideale (sinistro, destro, bilatero) B di A_1 e $f(f^{-1}(C)) = C \cap f(A_1)$ per ogni sottoanello o ideale (sinistro, destro, bilatero) C di A_2.

DIMOSTRAZIONE. (a) Dal teorema 6.16 segue che $f(H)$ è un sottogruppo di $(A_2, +)$. Se $a, b \in H$, allora $f(a)f(b) = f(ab) \in f(H)$, quindi $f(H)$ è sottoanello di A_2. Se A_1 e A_2 sono anelli unitari e f è un omomorfismo di anelli unitari si ha $f(1_A) = 1_B$. Pertanto $1_A \in H$ implica $1_B = f(1_A) \in f(H)$. Per $f^{-1}(C)$ si ragiona analogamente.

(b) Sia I un ideale sinistro di A_2. Dal teorema 6.16 segue che $f^{-1}(I)$ è un sottogruppo di $(A_1, +)$. Sia $a \in f^{-1}(I)$ cioè $f(a) \in I$. Se $x \in A_1$, allora $y = f(x) \in A_2$. Quindi $f(xa) = yf(a) \in I$. Questo significa $xa \in f^{-1}(I)$. Dunque $f^{-1}(I)$ è un ideale sinistro di A_1. Si ragiona analogamente quando I è un ideale destro o bilatero di A_2.

(c) Sia J un ideale sinistro di A_1. Il fatto che $f(J)$ è un sottogruppo di $(A_2, +)$ è stato già notato sopra. Sia $f(j) \in f(J)$, con $j \in J$. Sia $y \in f(A_1)$, allora esiste $x \in A_1$ con $f(x) = y$. Ora $xj \in J$ implica $yf(j) = f(x)f(j) = f(xj) \in f(J)$. Quindi $f(J)$ è un ideale sinistro di $f(A_1)$. Si ragiona analogamente quando J è un ideale destro o bilatero di A_1.

(d) Queste uguaglianze sono note dal caso degli omomorfismi di gruppo perché valgono per insiemi arbitrari B e C di A_1 e A_2 rispettivamente. □

Corollario 10.7. (Secondo teorema di omomorfismo per anelli) *Siano B un sottoanello e J un ideale bilatero di un anello A. Allora $B \cap J$ è un ideale bilatero di B e*

$$B/B \cap J \cong B + J/J.$$

DIMOSTRAZIONE. Consideriamo la restrizione $f = \pi|_B : B \to f(B)$ dell'omomorfismo $\pi : A \to A/J$. Poiché $B + J$ è un sottoanello di A per l'esercizio 9.16 e $f(B) = f(B + J)$, il sottoanello $f(B)$ coincide con il quoziente $B + J/J$. D'altra parte, $\ker f = \{x \in B : f(x) = 0\} = B \cap \ker \pi = B \cap J$. Per il primo teorema di omomorfismo 10.4 risulta $B/B \cap J \cong B + J/J$. □

Dimostriamo infine l'analogo del terzo teorema di omomorfismo 6.20 per i gruppi, in altre parole, per un ideale bilatero I di A_2 si ha $A_1/f^{-1}(I) \cong A_2/I$ qualora f sia suriettivo.

Teorema 10.8. *Siano A_1, A_2 anelli e $f : A_1 \to A_2$ un omomorfismo. Sia I un ideale bilatero di A_2 tale che $I \subseteq f(A_1)$. Allora*

$$A_1/f^{-1}(I) \cong f(A_1)/I.$$

In particolare $A_1/f^{-1}(I) \cong A_2/I$ quando f è suriettivo.

DIMOSTRAZIONE. Siano $\pi : f(A_1) \to f(A_1)/I$ la proiezione canonica relativa ad I e $g = \pi \circ f : A_1 \to f(A_1)/I$. Allora g è suriettiva e $\ker g = f^{-1}(I)$, da cui per il primo teorema di omomorfismo per gli anelli 10.4 risulta $A_1/f^{-1}(I) \cong f(A_1)/I$. In particolare $A_1/f^{-1}(I) \cong A_2/I$ quando f è suriettivo. □

Corollario 10.9. (Terzo teorema di omomorfismo per anelli) *Siano J, I ideali bilateri di un anello A e $I \subseteq J$. Allora J/I è un ideale bilatero di A/I e*

$$A/J \cong (A/I)/(J/I).$$

DIMOSTRAZIONE. Sia $\pi : A \to A/I$ la proiezione canonica relativa ad I. Per il punto (c) del teorema di corrispondenza 10.6 $\pi(J) = J/I$ è un ideale bilatero di A/I e $\pi^{-1}(J/I) = J$. Allora per il teorema 10.8 si ha $A/J \cong (A/I)/(J/I)$. □

Teorema 10.10. *Siano A_1, A_2 anelli commutativi unitari ed $f : A_1 \to A_2$ un omomorfismo. Sia I un ideale di A_2 tale che $I \subseteq f(A_1)$.*

(a) Se I è primo, allora $f^{-1}(I)$ è primo e contiene il nucleo di f.
(b) Se f è suriettivo e $f^{-1}(I)$ è primo (massimale), allora I è un ideale primo (rispettivamente massimale) di $f(A_1)$.

DIMOSTRAZIONE. Osserviamo che per il teorema 10.8, si ha $A_1/f^{-1}(I) \cong f(A_1)/I$.

(a) Se I è primo, allora A_2/I è un dominio per il teorema 9.29. Quindi anche $f(A_1)/I$ risulta un dominio in quanto sottoanello di un dominio. Per l'isomorfismo notato sopra e nuovamente per il teorema 9.29 concludiamo che l'ideale $f^{-1}(I)$ è primo.

(b) Supponiamo ora che $f^{-1}(I)$ sia primo. Il teorema 9.29 garantisce che $A_1/f^{-1}(I) \cong A_2/I$ risulta un dominio. Dunque I è primo. Se $f^{-1}(I)$ è massimale, allora il teorema 9.30 implica che $A_1/f^{-1}(I) \cong A_2/I$ è un campo, quindi l'ideale I di A_2 è massimale. □

Concludiamo con la seguente osservazione che sarà utile nel seguito.

Osservazione 10.11. Se $f : K \to A$ è un omomorfismo di anelli unitari e K è un campo, allora f è iniettivo. Infatti basta notare che $\ker f$ è un ideale proprio di K.

10.3 Anelli unitari e campo dei quozienti di un dominio

In questa sezione mostriamo come ogni anello si possa immergere in un anello unitario e come ogni anello commutativo senza divisori dello zero, in particolare ogni dominio, si possa immergere in un campo.

Teorema 10.12. *Sia A un anello, allora esiste un anello unitario B tale che A è isomorfo ad un ideale di B. Inoltre B è commutativo se e solo se A è commutativo.*

DIMOSTRAZIONE. Sia $B = A \times \mathbb{Z}$ il prodotto diretto dei gruppi abeliani $(A, +)$ e $(\mathbb{Z}, +)$ munito del prodotto

$$(a, n) \cdot (b, m) = (ab + ma + nb, nm), \text{ dove } a, b \in A, m, n \in \mathbb{Z}.$$

Si verifica facilmente che l'operazione $\cdot$ gode della proprietà associativa e delle due proprietà distributive rispetto alla somma. Vediamone una:

$$((a, n) + (a', n')) \cdot (b, m) = (a + a', n + n') \cdot (b, m) =$$
$$= ((a + a')b + m(a + a') + (n + n')b, (n + n')m) =$$
$$= ((ab + ma + nb) + (a'b + ma' + n'b), nm + n'm) =$$
$$= (ab+ma+nb, nm) + (a'b+ma' +n'b, n'm) = (a, n) \cdot (b, m) + (a', n') \cdot (b, m).$$

L'elemento $(0, 1)$ risulta essere l'elemento identico di B; infatti

$$(a, n) \cdot (0, 1) = (a, n) = (0, 1) \cdot (a, n),$$

per ogni $(a, n) \in B$. L'applicazione $f : A \to B$ definita da $f(a) = (a, 0)$ è un omomorfismo iniettivo di anelli di A in B. È sufficiente verificare che f "conserva" il prodotto, in quanto è già noto dalla teoria dei gruppi che f è un omomorfismo iniettivo di gruppi abeliani. Infatti

$$f(ab) = (ab, 0) = (a, 0) \cdot (b, 0) = f(a) \cdot f(b).$$

Possiamo pertanto identificare A con un sottoanello di B. Verifichiamo che in realtà A è un ideale bilatero di B. Siano $(a, 0) \in A$ e $(b, m) \in B$, si ha

$$(a, 0) \cdot (b, m) = (ab + ma, 0) \in A \quad \text{e} \quad (b, m) \cdot (a, 0) = (ba + ma, 0) \in A.$$

□

Non è difficile vedere che l'anello B costruito in questo modo può avere dei divisori dello zero anche quando A non ne ha. Per un esempio facile si consideri il caso $A = \mathbb{Z}$. Più in generale, per ogni dominio A l'estensione B ha divisori dello zero: per esempio l'elemento $(1_A, 0)$ di B risulta un divisore dello zero. Inoltre B può avere divisori dello zero anche quando A non è unitario e non ha divisori dello zero, si veda l'esercizio 10.1.

Ora vedremo che quando l'anello di partenza A è commutativo e senza divisori dello zero, allora A si può immergere in un campo.

Definizione 10.13. Sia A un anello commutativo integro. Un campo K si dice *campo dei quozienti* di A se esiste un omomorfismo iniettivo $f : A \to K$ di anelli tale che per ogni $x \in K$ esiste un elemento non nullo $b \in A$ con $f(b)x \in f(A)$.

In altre parole, ogni elemento x di K si può scrivere come una frazione o quoziente $f(a)f(b)^{-1}$, cioè K è il più piccolo campo che contiene A come suo sottoanello. Questo spiega il termine campo dei quozienti.

Teorema 10.14. *Sia A un anello commutativo privo di divisori di zero. Allora esiste un campo dei quozienti $f : A \to Q(A)$ di A.*

DIMOSTRAZIONE. Nell'insieme $A \times A^*$ introduciamo la relazione $(a, b) \sim (a', b')$ se $ab' = a'b$. Si verifica facilmente che questa è un relazione di equivalenza. Denotiamo con $Q(A)$ l'insieme delle classi di equivalenza. In particolare per $(a, b) \in A \times A^*$ denotiamo con $\frac{a}{b}$ la classe di equivalenza di (a, b). Introduciamo in $Q(A)$ due operazioni $+$ e $\cdot$ che lo renderanno un campo. Definiamo

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{e} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Si verifica facilmente che queste operazioni sono definite correttamente. Innanzitutto, poiché $b \neq 0 \neq d$ e A è privo di divisori di zero, si ha $bd \neq 0$. Verifichiamo ad esempio che l'operazione $+$ è ben definita. Supponiamo che

$$\frac{a}{b} = \frac{a'}{b'} \text{ e } \frac{c}{d} = \frac{c'}{d'}; \text{ allora } ab' = a'b, \;\; cd' = dc', \tag{1}$$

per come è stata definita la relazione di equivalenza. Dobbiamo verificare che

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ è uguale a } \frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd' + b'c'}{b'd'},$$

cioè che $(ad + bc)b'd' = (a'd' + b'c')bd$. Allora, usando (1)

$$(ad + bc)b'd' = adb'd' + bcb'd' = (ab')(dd') + (cd')(bb') =$$

$$= (a'b)(dd') + (c'd)(bb') = (a'd')(bd) + (b'c')(bd) = (a'd' + b'c')bd.$$

In modo analogo si dimostra che anche l'operazione $\cdot$ è ben definita. Si verifica inoltre che l'elemento $\frac{0}{b}$ è l'elemento neutro per la somma, che $\frac{-a}{b}$ è l'opposto di $\frac{a}{b}$ e che la somma gode delle proprietà associativa e commutativa. Pertanto $(Q(A), +)$ è un gruppo abeliano. Inoltre la moltiplicazione $\cdot$ rende $Q(A)$ un campo. Verifichiamo l'esistenza dell'identità e dell'inverso. Sia $c \in A^*$; allora l'elemento $\frac{c}{c}$ di $Q(A)$ (che ovviamente non dipende da c) è l'identità. Infatti

$$\frac{a}{b} \cdot \frac{c}{c} = \frac{ac}{bc} = \frac{a}{b},$$

poiché $(ac)b = a(cb) = a(bc)$. Sia ora $\frac{a}{b} \neq 0_{Q(A)}$, cioè $a \neq 0$. Allora $\frac{b}{a}$, la classe di equivalenza di $(b, a) \in A \times A^*$, è ben definita ed è l'inverso di $\frac{a}{b}$. Infatti

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab},$$

che abbiamo dimostrato essere l'identità.

Osserviamo ora che $\frac{ax}{x} = \frac{ay}{y}$ per ogni $x, y \in A^*$, in quanto $(ax)y = (ay)x$. Denotiamo pertanto con $f(a)$ la classe $\frac{ax}{x}$ per ogni $a \in A$ e $x \in A^*$ e troviamo l'omomorfismo desiderato. Infatti, per qualche $x \in A^*$ si ha

$$f(a) + f(b) = \frac{ax}{x} + \frac{bx}{x} = \frac{ax^2 + bx^2}{x^2} = \frac{(a+b)x^2}{x^2} = f(a+b).$$

Infine f è iniettivo, in quanto $f(a) = f(b)$ implica $(ax)x = (bx)x$ per qualche $x \in A^*$, da cui si conclude $a = b$ per il fatto che A è un dominio. □

Osserviamo che se identifichiamo A con la sua immagine $f(A)$ in Q, allora

$$\frac{a}{b} = a \cdot b^{-1} \text{ in } Q(A),$$

per ogni $a, b \in A$, $b \neq 0$.

Se A è un dominio, la dimostrazione si semplifica, come illustriamo nell'osservazione 10.15. Tuttavia è preferibile avere il teorema nel caso generale, perché per un anello commutativo non unitario A senza divisori dello zero non si può sperare di applicare prima il teorema 10.12 trovando un dominio B al quale applicare poi il teorema 10.14.

Osservazione 10.15. La dimostrazione del teorema 10.14 si può semplificare nel caso di un dominio. In tal caso l'immersione f di A in $Q(A)$ si può definire semplicemente con $f(a) = \frac{a}{1}$ per $a \in A$ e l'inverso di a (più precisamente di $f(a)$) in $Q(A)$ sarà $\frac{1}{a}$ (più precisamente, $\frac{1}{f(a)}$). Infine l'identità $1_{Q(A)}$ coincide con $f(1_A)$.

Dimostriamo che il campo dei quozienti di un dominio è unico a meno di isomorfismo.

Teorema 10.16. *Sia A un dominio e sia $f : A \to Q(A)$ un suo campo dei quozienti. Se K è un campo e $g : A \to K$ è un omomorfismo iniettivo di anelli unitari, allora esiste un unico omomorfismo di anelli unitari $h : Q(A) \to K$, tale che $h \circ f = g$.*

DIMOSTRAZIONE. Ponendo

$$h\left(\frac{a}{b}\right) = g(a) \cdot g(b)^{-1}$$

si ottiene l'omomorfismo di anelli $h : Q(A) \to K$ desiderato. Infatti questa definizione è corretta in quanto l'iniettività di g implica $g(b) \neq 0$ e quindi esiste $g(b)^{-1} \in K$. Inoltre, essa non dipende della scelta di $a, b \in A$ in quanto $\frac{a}{b} = \frac{a_1}{b_1}$ in $Q(A)$ implica $ab_1 = a_1 b$ in A e quindi $g(a)g(b_1) = g(a_1)g(b)$ in K. Pertanto $g(a) \cdot g(b)^{-1} = g(a_1) \cdot g(b_1)^{-1}$ in K. Questo dimostra anche l'unicità di h. □

Notiamo che l'omomorfismo h nel teorema è iniettivo per l'osservazione 10.11.

Corollario 10.17. *Sia A un dominio e siano $f_1 : A \to Q_1(A)$ e $f_2 : A \to Q_2(A)$ due suoi campi dei quozienti. Allora esiste un isomorfismo di anelli unitari*

$$i : Q_1(A) \to Q_2(A), \quad \textit{tale che } i \circ f_1 = f_2.$$

DIMOSTRAZIONE. Applichiamo al campo dei quozienti $f_1 : A \to Q_1(A)$ e all'omomorfismo f_2 il teorema 10.16. Si ottiene un omomorfismo iniettivo h_1 da $Q_1(A)$ in $Q_2(A)$ con $h_1 \circ f_1 = f_2$. Analogamente, applichiamo il teorema 10.16 al campo di quozienti $f_2 : A \to Q_2(A)$ e all'omomorfismo f_1: si ottiene ora un omomorfismo iniettivo $h_2 : Q_2(A) \to Q_1(A)$ con $h_2 \circ f_2 = f_1$. Ora l'unicità dal teorema 10.16, applicata al campo di quozienti $f_2 : A \to Q_2(A)$ e agli omomorfismi $h_1 \circ h_2 : Q_2(A) \to Q_2(A)$ e $id_{Q_2(A)} : Q_2(A) \to Q_2(A)$ che soddisfano $h_1 \circ h_2 \circ f_2 = f_2 = id_{Q_2(A)} \circ f_2$ permette di concludere che $h_1 \circ h_2 = id_{Q_2(A)}$. Analogamente $h_2 \circ h_1 = id_{Q_1(A)}$. Quindi h_1 e h_2 sono isomorfismi. □

In altre parole, il corollario dice che se identifichiamo il dominio A con la sua immagine $f_\nu(A)$ in $Q_\nu(A)$, per $\nu = 1, 2$, allora esiste un isomorfismo di anelli $i : Q_1(A) \to Q_2(A)$ che non muove gli elementi di A, ovvero $i(a) = a$ per ogni $a \in A$.

10.4 Prodotto diretto di anelli

Dati due anelli A e B, possiamo definire il prodotto diretto $A \times B$ dei gruppi abeliani $(A, +, 0_A)$ e $(B, +, 0_B)$ e su questo definire un prodotto nel modo seguente:

$$(a, b) \cdot (a', b') = (aa', bb'), \text{ dove } a, a' \in A, b, b' \in B.$$

Abbiamo dimostrato nel teorema 4.19 che $(A \times B, +, \cdot, (0_A, 0_B))$ risulta un anello, che scriveremo brevemente $A \times B$ e chiameremo *prodotto diretto* di A e B.

Teorema 10.18. *Siano A e B anelli. Allora $(A \times B, +, \cdot, (0_A, 0_B))$ risulta un anello. Se A e B sono anelli unitari, allora $(1_A, 1_B)$ è l'unità di $A \times B$.*

DIMOSTRAZIONE. Dal teorema 4.19 (c) segue che $(A \times B, +, (0_A, 0_B))$ risulta un anello. Verifichiamo che $(1_A, 1_B)$ è l'unità di $A \times B$ nel caso in cui A e B siano anelli unitari. Per ogni coppia $(a, b) \in A \times B$ risulta

$$(1_A, 1_B)(a, b) = (1_A a, 1_B b) = (a, b) = (a 1_A, b 1_B) = (a, b)(1_A, 1_B).$$

□

Siano $p_1 : A \times B \to A$ e $p_2 : A \times B \to B$ le due proiezioni definite da $p_1((a, b)) = a$ e $p_2((a, b)) = b$. Allora p_1 e p_2 sono omomorfismi di anello. Infatti, per $a, a_1 \in A$ e $b, b_1 \in B$ si ha

$$p_1((a, b)(a_1, b_1)) = p_1((aa_1, bb_1)) = aa_1 = p_1((a, b))p_1((a_1, b_1)).$$

Analogamente si dimostra che p_2 è un omomorfismo. Ora i nuclei $B_1 = \ker p_1$ e $A_1 = \ker p_2$ sono ideali bilateri di $A \times B$. Questo si vede facilmente anche dalla forma esplicita

$$B_1 = \{(0_A, b) : b \in B\} = \{0_A\} \times B \quad \text{e} \quad A_1 = \{(a, 0_B) : a \in A\} = A \times \{0_B\}.$$

Inoltre $i : B_1 \to B$ e $j : A_1 \to A$ definiti da $i(0, b) = b$ e $j(a, 0) = a$ sono isomorfismi che permettono di identificare gli anelli A e B con gli ideali bilateri A_1 e B_1, rispettivamente, del prodotto diretto $R = A \times B$.

Notiamo infine che sono verificate anche le condizioni:

(1) $A_1 \cap B_1 = \{0\}$, e
(2) $R = A_1 + B_1$.

Infatti (1) è ovvia. Per (2) basta notare che se $(a, b) \in A \times B$, allora

$$(a, b) = (a, 0_B) + (0_A, b).$$

Possiamo scrivere anche $(a, b) = (0_A, b) + (a, 0_B)$, poiché $(A \times B, +)$ è prodotto diretto dei gruppi abeliani $(A, +)$ e $(B, +)$.

Definizione 10.19. Un elemento i di un anello A si dice *idempotente* se $i = i^2$. Se inoltre i commuta con tutti gli elementi di A si dice *idempotente centrale.*

Se A è unitario, due idempotenti i, j si dicono *ortogonali* se

$$i + j = 1_A \quad \text{e} \quad ij = ji = 0.$$

In una coppia di idempotenti centrali ortogonali i, j ognuno determina l'altro tramite l'uguaglianza $i + j = 1$. In altre parole, ogni idempotente i dà luogo alla coppia $i, 1 - i$ di idempotenti ortogonali. Inoltre $1 - i$ è centrale se e solo se i è centrale.

È facile vedere che se il prodotto diretto $R = A \times B$ è un anello unitario, allora ognuno degli anelli A e B è unitario e gli elementi $i = (1_A, 0_B)$ e $j = (0_A, 1_B)$ sono idempotenti centrali ortogonali.

Teorema 10.20. *Sia R un anello e siano A e B due ideali bilateri di R tali che $A \cap B = \{0\}$ e $R = A + B$. Allora R è isomorfo al prodotto diretto $A \times B$. Inoltre*

(a) se R è unitario, allora A e B sono generati da elementi idempotenti centrali ortogonali;

(b) se A e B sono generati da elementi idempotenti centrali i e j rispettivamente, allora R è unitario con unità $i + j$, cioè i e j sono ortogonali.

DIMOSTRAZIONE. Da $A \cap B = \{0\}$ e $R = A + B$ concludiamo che $R \cong A \times B$ come gruppo abeliano. Inoltre, da $A \cap B = \{0\}$ si ha

$$(a + b)(a_1 + b_1) = aa_1 + ab_1 + ba_1 + bb_1 = aa_1 + bb_1$$

per $a, a_1 \in A$ e $b, b_1 \in B$. Quindi l'isomorfismo $R \cong A \times B$ è anche un isomorfismo di anelli.

(a) Supponiamo che R sia unitario. Allora $1 = i + j$, con $i \in A$ e $j \in B$. Da $1^2 = 1$ ricaviamo $1 = i^2 + j^2 = i + j$. Pertanto $A \cap B = \{0\}$ implica $i^2 = i$ e $j^2 = j$. Ora per $r \in R$ sia ha $r \cdot 1 = 1 \cdot r$, quindi $ri + rj = ir + jr$. Dunque $ri - ir = jr - rj \in A \cap B = \{0\}$. Quindi $ri = ir$ e $jr = rj$. Questo dimostra che i e j sono idempotenti centrali ortogonali. Si ha $(i) \subseteq A$ e $(j) \subseteq B$. Essendo $(i) + (j)$ un ideale bilatero contenente 1, si ha $R = (i) + (j)$. Questo implica $A = (i)$ e $B = (j)$.

(b) Supponiamo che gli ideali A e B siano generati da elementi idempotenti centrali i e j rispettivamente. Consideriamo l'elemento $r = i + j$ di R. Per ogni $x = a + b \in R$ si ha $a = ai$ e $b = bj$ poiché $A = (i)$ e $B = (j)$. Infatti $a \in A = (i)$ implica che esiste $c \in R$ tale che $a = ci$, da cui $ai = ci^2 = ci = a$ e così per b. Quindi $xr = ai + bj = x$. Analogamente si vede che $rx = x$. Dunque r è l'unità di R. □

Il prodotto diretto di tre o più anelli si definisce in modo analogo. I dettagli si possono vedere negli esercizi, in particolare l'esercizio 10.42 (o) illustra anche un esempio di anello B isomorfo a $B \times B$.

Calcoliamo ora la caratteristica del prodotto diretto di due anelli unitari.

Teorema 10.21. *Siano A e B due anelli unitari. Allora per il prodotto diretto*

$$R = A \times B$$

si ha

(a) char $R = 0$ *se* char $A = 0$ *o* char $B = 0$*;*

(b) se char $A \neq 0 \neq$ char B*, allora* char R *coincide con il minimo comune multiplo di* char A *e* char B*.*

Dimostrazione. (a) Se char$A = 0$, allora per l'unità $1 = (1_A, 1_B)$ di R si ha $m \cdot 1 = (m \cdot 1_A, m \cdot 1_B) \neq 0$, in quanto $m \cdot 1_A \neq 0$ per ogni $m > 0$. Questo dimostra char$R = 0$. In modo analogo si ragiona quando char$B = 0$.

(b) Supponiamo char$A = m > 0$ e char$B = n > 0$. Allora l'elemento 1_A del gruppo abeliano $(A, +)$ ha periodo m, mentre l'elemento 1_B del gruppo abeliano $(B, +)$ ha periodo n. Quindi il periodo dell'elemento $1 = (1_A, 1_B)$ del gruppo abeliano $(R, +) = (A, +) \times (B, +)$ coincide con il minimo comune multiplo di m e n, per la proposizione 6.40. □

10.5 Reticoli e algebre di Boole

In questo paragrafo studieremo altre strutture algebriche con due operazioni binarie. Ricordiamo che un reticolo è un insieme ordinato $(L, \leq)$ tale che per ogni coppia $a, b \in L$ l'insieme $\{a, b\}$ ammette estremo superiore, denotato con $a \vee b$, e estremo inferiore, denotato con $a \wedge b$. Questo permette di considerare $\wedge$ e $\vee$ come due operazioni binarie sull'insieme supporto L che permettono poi di recuperare facilmente

l'ordine originale di L, perché $a \leq b$ se e solo se $a = a \wedge b$ se e solo se $b = a \vee b$. Nel seguito denoteremo con $(L, \wedge, \vee)$ un reticolo per mettere in evidenza le operazioni $\wedge$ e $\vee$. È facile verificare che in ogni reticolo valgono la legge commutativa e la legge associativa per entrambe le operazioni, cioè

$$x \wedge y = y \wedge x, \quad (x \wedge y) \wedge z = x \wedge (y \wedge z),$$

$$x \vee y = y \vee x, \quad (x \vee y) \vee z = x \vee (y \vee z)$$

per ogni $x, y, z \in L$. Inoltre, se L è limitato, allora 0 è l'elemento neutro per l'operazione $\vee$, mentre 1 è l'elemento neutro per l'operazione $\wedge$. Denoteremo con $(L, \wedge, \vee, 0, 1)$ un reticolo limitato. Un sottoinsieme M di un reticolo $(L, \wedge, \vee)$ si dice un *sottoreticolo* se $a \wedge b \in M$ e $a \vee b \in M$ per ogni $a, b \in M$.

Definizione 10.22. Siano $(L_1, \wedge, \vee)$ e $(L_2, \wedge, \vee)$ due reticoli. Allora un'applicazione $f : L_1 \longrightarrow L_2$ si dice un *omomorfismo di reticoli*, se

$$f(a \wedge b) = f(a) \wedge f(b) \quad \text{e} \quad f(a \vee b) = f(a) \vee f(b)$$

per tutti gli $a, b \in L_1$. Se f è biettiva, f si dice un *isomorfismo di reticoli*. Se L_1 ed L_2 sono reticoli limitati con 0_i e 1_i il minimo e il massimo di L_i, $i = 1, 2$, allora f si dice un *omomorfismo di reticoli limitati* se $f(1_1) = 1_2$ e $f(0_1) = 0_2$.

Lasciamo per esercizio la dimostrazione della seguente proprietà.

Proposizione 10.23. *Siano $(L, \wedge, \vee, 0, 1)$ un reticolo limitato e $x, y, z \in L$. Allora le seguenti affermazioni sono equivalenti:*

(a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$,
(b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Un reticolo che soddisfi una delle condizioni equivalenti della precedente proposizione 10.23 si dice un reticolo *distributivo*.

Definizione 10.24. Sia $(L, \wedge, \vee, 0, 1)$ un reticolo limitato:

- un elemento $a \in X$ si dice *complemento* di un elemento b se $a \vee b = 1$ e $a \wedge b = 0$;
- un reticolo limitato si dice *complementato* se ogni suo elemento ammette complemento;
- un reticolo distributivo e complementato si dice *reticolo di Boole* o *reticolo Booleano*.

Si verifica facilmente che se un elemento di un reticolo limitato distributivo ammette complemento, tale complemento è unico, si veda l'esercizio 10.34. D'ora in avanti denoteremo con $\overline{x}$ l'unico complemento di x. Non è difficile verificare che in un reticolo di Boole valgono le *leggi di De Morgan*:

$$\overline{x \vee y} = \overline{x} \wedge \overline{y} \quad \text{e} \quad \overline{x \wedge y} = \overline{x} \vee \overline{y}.$$

Esempio 10.25. (a) L'insieme ordinato $\mathbb{B} = \{0, 1\}$, con $0 < 1$, ammette un'unica struttura di reticolo che lo rende un reticolo Booleano. Ogni reticolo Booleano contiene una copia di $\mathbb{B}$.

(b) Per ogni insieme non vuoto X l'insieme parzialmente ordinato $(\mathcal{P}(X), \subseteq)$ risulta un reticolo Booleano, con $1 = X, 0 = \emptyset, A \vee B = A \cup B, A \wedge B = A \cap B$ per $A, B \in \mathcal{P}(X)$. Di conseguenza ogni sottoreticolo di $\mathcal{P}(X)$ risulta distributivo. Vedremo nel teorema 10.33 che ogni reticolo distributivo limitato ha questa forma, cioè è isomorfo a qualche sottoreticolo di $\mathcal{P}(X)$ per un opportuno insieme X.

Lemma 10.26. *Un insieme totalmente ordinato è un reticolo di Boole se e solo se coincide con* $\mathbb{B}$.

DIMOSTRAZIONE. Se un insieme totalmente ordinato ha due elementi x e y, allora $x < y$ e x sarà il minimo e y il massimo.

Supponiamo ora che un insieme totalmente ordinato sia un reticolo di Boole con minimo 0 e massimo 1. Sia x un elemento di X; allora esiste un complemento y di x, cioè esiste y tale che $x \wedge y = 0$ e $x \vee y = 1$. Poiché X è totalmente ordinato, si avrà $x \leq y$ oppure $y \leq x$. Nel primo caso $0 = x \wedge y = x$, nel secondo caso $1 = x \vee y = x$. Pertanto $X = \{0, 1\}$. □

Ricordiamo il lemma di Zorn.

Lemma di Zorn. *Ogni insieme parzialmente ordinato e induttivo ammette elementi massimali.*

Il lemma di Zorn è stato essenziale nella dimostrazione del teorema di Krull 9.33. Nel seguente teorema 10.32 e negli esercizi 10.36, 10.39 vedremo altre applicazioni tipiche del lemma di Zorn.

Definizione 10.27. Sia $(L, \wedge, \vee, 0, 1)$ un reticolo limitato. Un *ideale* di L è un sottoinsieme non vuoto I di L con le proprietà:

(a) $1 \notin I$;
(b) se $a \in I$ e $b \leq a$ allora anche $b \in I$;
(c) se $a, b \in I$, allora anche $a \vee b \in I$.

Per $a \in L$ poniamo $\downarrow a := \{x \in L : x \leq a\}$; allora $\downarrow a$ è il più piccolo ideale di L contenente a. Lo chiameremo *ideale principale* generato da a.

Lemma 10.28. *Ogni ideale di un reticolo finito L è principale.*

DIMOSTRAZIONE. Sia m un elemento dell'ideale I che sia massimale per I: un tale elemento esiste poiché L è finito. Dimostriamo che $I = \downarrow m$: infatti se $a \in I$, allora $a \vee m \in I$ e $m \leq a \vee m$, quindi per la scelta di m si ha $m = a \vee m$ e di conseguenza $a \leq m$. □

Esempio 10.29. Per ogni insieme infinito X il reticolo Booleano $\mathcal{P}(X)$ ha ideali non principali. Per esempio la famiglia I_∞ di tutti i sottoinsiemi finiti di X è un ideale non principale di $\mathcal{P}(X)$. Infatti se fosse $I_\infty = \downarrow Y$ per qualche $Y \subseteq X$, si avrebbe $I_\infty = \{Z \in \mathcal{P}(X) : Z \subseteq Y\} = \mathcal{P}(Y)$. In particolare $Y \in I_\infty$ da cui segue che Y sarebbe finito e quindi anche I_∞ sarebbe finito. Se X è infinito, allora l'insieme dei singoletti $\{x\}$ è infinito e contenuto in I_∞, contraddicendo l'ultima affermazione

Definizione 10.30. Sia $(L, \wedge, \vee, 0, 1)$ un reticolo distributivo limitato. Denotiamo con $\mathcal{J}(L)$ l'insieme degli ideali di L.

Osserviamo che $\mathcal{J}(L)$ è un sottoinsieme di $\mathcal{P}(L)$, l'insieme parti di L, ed è quindi ordinato con l'ordine indotto da $\mathcal{P}(L)$, cioè diremo che $I \leq J$ per due ideali se $I \subseteq J$.

Definizione 10.31. Un ideale I di L è *primo* se $a \wedge b \in I$ implica $a \in I$ oppure $b \in I$.

Lemma 10.32. *Siano L un reticolo distributivo, $x, y \in L$ con $y \not\leq x$. Allora esiste un ideale primo di L che contiene x ma non contiene y.*

DIMOSTRAZIONE. Sia $\mathcal{I}$ l'insieme degli ideali di L che contengono x e non contengono y. L'insieme $\mathcal{I}$ non è vuoto perché contiene $\downarrow x$ e l'insieme ordinato $(\mathcal{I}, \leq)$ è induttivo. Per il lemma di Zorn esiste un elemento massimale M di $\mathcal{I}$. Per vedere che M è primo supponiamo che esistano $a, b \in L$ con $a \wedge b \in M$, ma $a \notin M$ e $b \notin M$. Sia M_a l'insieme degli elementi u di L tale che esiste $m \in M$ con $u \leq a \vee m$. Siano $u, v \in M_a$, e $t \in L$ con $t \leq u$, allora $t \in M_a$. Inoltre se $u \leq a \vee m$ e $v \leq a \vee n$ con $n, m \in M$, allora $u \vee v \leq a \vee (n \vee m)$ con $n \vee m \in M$, in quanto M è un ideale. Infine se per assurdo $1 \in M_a$, si avrebbe $1 = a \vee m$, per qualche $m \in M$. Allora

$$m \vee (a \wedge b) = (m \vee a) \wedge (m \vee b) = 1 \wedge (m \vee b) = m \vee b$$

è un elemento di M e quindi anche $b \leq m \vee b$ è un elemento di M, in quanto M è un ideale, ma questo contraddice l'ipotesi $b \notin M$. Pertanto $1 \notin M_a$ e M_a è un ideale che contiene M. Osserviamo che $a \leq a \vee (a \wedge b)$, da cui segue $a \in M_a$. Allora M_a è un ideale di L che contiene propriamente M, e quindi $M_a \notin \mathcal{I}$, cioè $y \in M_a$, e di conseguenza $y \leq a \vee m_1$ per qualche elemento $m_1 \in M$. Analogamente risulta $y \leq b \wedge m_2$ per qualche elemento $m_2 \in M$. Dunque

$$y = y \wedge y \leq (a \vee m_1) \wedge (b \vee m_2) = (a \wedge b) \vee (a \wedge m_2) \vee (m_1 \wedge b) \vee (m_1 \wedge m_2) \in M,$$

assurdo. □

Ora possiamo dare il teorema di rappresentazione dei reticoli distributivi limitati.

Teorema 10.33. *Ogni reticolo distributivo limitato L è isomorfo ad un sottoreticolo di un reticolo del tipo $\mathcal{P}(X)$.*

DIMOSTRAZIONE. Sia X l'insieme degli ideali primi di L. All'elemento $x \in L$ si mette in corrispondenza l'insieme P_x degli ideali primi di L che non contengono x.

Consideriamo l'applicazione $\varphi : L \to \mathcal{P}(X)$ definita da $\varphi(x) := P_x$. Si deduce facilmente dalla definizione di φ, che $\varphi(0) = \emptyset$, $\varphi(1) = X$. Vale

$$\varphi(x \vee y) = P_{x \vee y} = P_x \cup P_y$$

in quanto se $I \in P_x$, si ha $I \in P_{x \vee y}$ e analogamente se $I \in P_y$. Viceversa se $I \in P_{x \vee y}$ allora $x \vee y \notin I$ e se $x \in I$, allora $y \notin I$, altrimenti ci starebbe anche $x \vee y$. Da questo segue che $I \in P_x \cup P_y$. Inoltre

$$\varphi(x \wedge y) = P_{x \wedge y} = P_x \cap P_y.$$

Infatti se $I \in P_{x \wedge y}$, allora $I \in P_x$ e $I \in P_y$. Viceversa se $I \in P_x \cap P_y$ si ha che $x \notin I$ e $y \notin I$, ma allora poiché I è un ideale primo $x \wedge y \notin I$, da cui $I \in P_{x \wedge y}$. Pertanto φ è un omomorfismo di reticoli tra L e $\varphi(L)$, quindi $\varphi(L)$ è un sottoreticolo di $\mathcal{P}(X)$. Segue dal lemma 10.32 che $\varphi : L \to \mathcal{P}(X)$ è iniettiva. Dunque L è isomorfo al sottoreticolo $\varphi(L)$ di $\mathcal{P}(X)$. □

Se L è un reticolo Booleano allora l'isomorfismo $\varphi : L \to \mathcal{P}(X)$ costruito nella dimostrazione del teorema 10.33 soddisfa $\varphi(\overline{x}) = X \setminus \varphi(x)$. In altre parole, oltre alle due operazioni reticolari φ è compatibile anche con il complemento. Il reticolo Booleano $\mathcal{P}(X)$ ammette una struttura di anello unitario (si veda l'esercizio 10.10) che induce anche su L una struttura di anello unitario, oltre a quella di reticolo. Per questo motivo, quando visto sotto questo aspetto, un reticolo Booleano, munito della struttura di anello unitario si dice spesso anche anello Booleano, o *algebra di Boole*, si veda anche l'esercizio 10.33.

Per motivi storici X si chiama *spettro* del reticolo L e si denota con Spec L. La rappresentazione di L tramite sottoinsiemi di Spec L è nota come *dualità di Stone*.

10.6 Esercizi su omomorfismi e prodotti diretti di anelli

Esercizio 10.1 Dimostrare con un esempio che l'anello B definito nel teorema 10.12 può avere divisori dello zero anche se A non ha divisori dello zero.

Esercizio 10.2 Verificare che la composizione di omomorfismi è un omomorfismo.

Esercizio 10.3 Sia A un anello e sia $a \in U(A)$. Si dimostri che

(a) l'applicazione $\varphi_a : A \to A$ definita da $\varphi_a(x) = a^{-1}xa$ è un omomorfismo di anelli;
(b) per $a, b \in U(A)$ si ha $\varphi_a \circ \varphi_b = \varphi_{ba}$;
(c) φ_a è un isomorfismo per ogni a.

Esercizio 10.4 Usando il teorema di corrispondenza 10.6, dare una nuova dimostrazione del teorema 9.30.

Esercizio 10.5 Siano G gruppo abeliano ed $A = End(G)$ l'insieme degli endomorfismi di G. Siano $f, g \in A$ e si definisca la somma $(f + g)(x) = f(x) + g(x)$, per $x \in G$. Sia $\circ$ l'usuale composizione di funzioni, cioè $(f \circ g)(x) = f(g(x))$ per $x \in G$. Si dimostri che $(A, +, \circ, id_A)$ è un anello unitario.

Esercizio 10.6 * Sia A un anello unitario. Dimostrare che A si può identificare con un sottoanello dell'anello $End(G)$ per qualche gruppo abeliano G, con $End(G)$ anello degli endomorfismi di G, definito nell'esercizio 10.5.

Esercizio 10.7 Siano G un gruppo abeliano ed $End(G)$ il suo anello degli endomorfismi, definito nell'esercizio 10.5. Dimostrare che

(a) $End(\mathbb{Z}^2)$ è isomorfo all'anello $M_2(\mathbb{Z})$;
(b) $End(\mathbb{Z}_m^2)$ è isomorfo all'anello $M_2(\mathbb{Z}_m)$ per ogni $m > 1$;
(c) $End(\mathbb{Q}^2)$ è isomorfo all'anello $M_2(\mathbb{Q})$.

Esercizio 10.8 Sia G un gruppo abeliano, $A = End(G)$ e sia $f \in A$ un endomorfismo. Dimostrare che:

(a) se f è suriettivo, allora f non è divisore dello zero destro;
(b) se f è iniettivo, allora f non è divisore dello zero sinistro.

Esercizio 10.9 È vero che un divisore dello zero destro risulta sempre anche un divisore dello zero sinistro in ogni anello?

Esercizio 10.10 Sia S un insieme. Nell'insieme $\mathcal{P}(S)$ si definisce l'operazione $\triangle$ (differenza simmetrica):

$$X \triangle Y = (X \cup Y) \setminus (X \cap Y)$$

per ogni coppia (X, Y) di sottoinsiemi di S.

(a) Provare che la struttura algebrica $A = (\mathcal{P}(S), \triangle, \cap)$ è un anello commutativo unitario e che ogni sottoinsieme proprio di S è divisore dello zero di A.
(b) Sia $Y \in \mathcal{P}(S)$; provare che l'applicazione $\varphi : \mathcal{P}(S) \to \mathcal{P}(S)$, definita da $\varphi(X) = X \setminus Y$ è un omomorfismo di anelli e determinare $\ker \varphi$ e $\operatorname{Im} \varphi$.
(c) Sia $Y \in \mathcal{P}(S)$; determinare l'ideale (Y).
(d) Se S è finito, provare che ogni ideale di $\mathcal{P}(S)$ è principale.
(e) Determinare la caratteristica di $\mathcal{P}(S)$.

Esercizio 10.11 Sia

$$B = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C}, \right\}$$

sottoinsieme dell'anello $M_2(\mathbb{C})$.

(a) Provare che B è un sottoanello di $M_2(\mathbb{C})$.
(b) Sia $q = a + bi + cj + dk$ un elemento del corpo dei quaternioni $\mathbb{H}$. Si dimostri che l'applicazione $\varphi : \mathbb{H} \to B$ definita da

$$\varphi(q) = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \quad \text{con} \quad \alpha = a + bi, \quad \beta = c + di \in \mathbb{C}$$

è un isomorfismo di anelli e pertanto di corpi.

(c) Si verifichi che

$$\det(\varphi(q)) = \|q\|^2 = a^2 + b^2 + c^2 + d^2.$$

Si deduca che

$$\|q \cdot q_1\| = \|q\| \cdot \|q_1\| \text{ per ogni } q, q_1 \in \mathbb{H}.$$

(d) Si verifichi che l'insieme dei quaternioni di norma 1 è un sottogruppo del gruppo moltiplicativo $(\mathbb{H} \setminus \{0\}, \cdot)$.

Esercizio 10.12 Determinare tutti gli endomorfismi φ di anello:

(a) $\varphi : \mathbb{Z} \to \mathbb{Z}$;
(b) $\varphi : \mathbb{Q} \to \mathbb{Q}$;
(c) $\varphi : \mathbb{R} \to \mathbb{R}$;
(d) $\varphi : \mathbb{Z}[i] \to \mathbb{Z}[i]$;
(e) $\varphi : \mathbb{Z}[\sqrt{n}] \to \mathbb{Z}[\sqrt{n}]$.

Esercizio 10.13 Siano A_1, A_2 anelli unitari e $f : A_1 \to A_2$ un omomorfismo suriettivo di anelli unitari.

(a) Provare che $f(U(A_1)) \subseteq U(A_2)$.
(b) Considerando l'omomorfismo $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(z) = z + n\mathbb{Z}$, mostrare che in (a) non vale l'uguaglianza se $n > 6$.

Esercizio 10.14 Nell'anello $M_2(\mathbb{Z})$ si consideri l'insieme

$$A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a \in \mathbb{Z}, b \in 3\mathbb{Z} \right\}.$$

(a) Verificare che A è sottoanello di $M_2(\mathbb{Z})$.
(b) Provare che l'applicazione $f : A \to \mathbb{Z}_9$, definita da $\begin{pmatrix} a & b \\ b & a \end{pmatrix} \mapsto a + 9\mathbb{Z}$ è un omomorfismo di anelli.
(c) Determinare il nucleo I di f. Dire se I è un ideale principale di A.

Esercizio 10.15 Siano A e B due campi. È vero che $A \times B$ è un campo?

Esercizio 10.16 Sia A l'anello $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$.

(a) Trovare la caratteristica di A.
(b) Descrivere gli ideali di A. In particolare determinare gli ideali primi e quelli massimali. Determinare se esistono ideali non principali.
(c) Determinare a quale degli anelli $\mathbb{Z}_4 \times \mathbb{Z}_{15}$, $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ e $\mathbb{Z}_{60}$ è isomorfo l'anello A.
(d) Descrivere quali sono gli elementi invertibili e gli elementi nilpotenti di A.

Esercizio 10.17 Sia $A_1 \times A_2$ il prodotto diretto di due anelli A_1 e A_2. Si provi che

(a) $(A_1 \times A_2, +, \cdot)$ è anello commutativo se e solo se A_1 e A_2 sono commutativi.
(b) $U(A_1 \times A_2) = U(A_1) \times U(A_2)$.

(c) Calcolare $U(\mathbb{Z}_2 \times \mathbb{Z}_5)$, $U(\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7)$, $U(\mathbb{Z}_4 \times \mathbb{Z}_6)$.

Esercizio 10.18 Siano A, B anelli commutativi unitari ed I un ideale di $C = A \times B$. Identifichiamo A con l'ideale $A \times \{0\}$ di C e B con l'ideale $\{0\} \times B$ di C. Provare che:

(a) $I = I_1 \times I_2$, dove I_1 è un ideale di A e I_2 è un ideale di B;
(b) $C/I \cong A/I_1 \times B/I_2$;
(c) se I è primo, allora o $I_1 = A$ e I_2 è un ideale primo di B, o $I_2 = B$ e I_1 è un ideale primo di A;
(d) se I_1 è un ideale primo di A, allora $I = I_1 \times B$ è un ideale primo di C;
(e) se I è massimale, allora o $I_1 = A$ e I_2 è un ideale massimale di B, o $I_2 = B$ e I_1 è un ideale massimale di A;
(f) se I_1 è un ideale massimale di A, allora $I = I_1 \times B$ è un ideale massimale di C;
(g) se A e B sono anelli a ideali principali, allora anche C è anello a ideali principali.

Esercizio 10.19 Determinare gli ideali di $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_6$.

Esercizio 10.20 Sia K un campo e $A = K \times K \times \cdots \times K$ (n fattori). Quali sono gli ideali primi di A? Quali sono gli ideali massimali di A?

Esercizio 10.21 Siano A un anello commutativo unitario, $n \in \mathbb{N}, n \geq 2$ e siano I_1, $I_2, \ldots, I_n$ ideali di A con $I_j + I_k = A$ per $1 \leq j < k \leq n$. Dimostrare che

$$A/\bigcap_{k=1}^{n} I_k \cong A/I_1 \times A/I_2 \times \ldots \times A/I_n.$$

Esercizio 10.22 Siano A un anello commutativo unitario, $n \in \mathbb{N}$, $n \geq 2$ e M_1, $M_2, \ldots, M_n$ ideali massimali a due a due distinti di A. Allora per ogni n-upla $(k_1, k_2, \ldots, k_n)$ di numeri interi positivi si ha

$$A/\bigcap_{i=1}^{n} M_i^{k_i} \cong A/M_1^{k_1} \times A/M_2^{k_2} \times \ldots \times A/M_n^{k_n}.$$

Esercizio 10.23* Dimostrare che ogni anello commutativo unitario finito è prodotto diretto di anelli locali.

Esercizio 10.24 Siano G un gruppo finito con elemento neutro e, R un anello e e $R[G]$ l'anello gruppale definito nell'esercizio 9.20. Dati due monoidi M ed N, un'applicazione $f : M \to N$ si dice un *omomorfismo di monoidi* se $f(1_M) = 1_N$ e $f(ab) = f(a)f(b)$ per ogni $a, b \in M$.

(a) Dimostrare che l'applicazione $\iota_R : R \to R[G]$ definita da

$$\iota_R(r) = re, \quad r \in R$$

è un omomorfismo iniettivo di anelli. Se R è unitario, ι_R è un omomorfismo di anelli unitari.

(b) Nel seguito supponiamo che R sia unitario. Dimostrare che l'applicazione $\iota_G : G \to R[G]$ definita da

$$\iota_G(g) = 1_R g, \quad g \in G$$

è un omomorfismo iniettivo di monoidi. Identifichiamo G con la sua immagine $\iota_G(G)$ in $R[G]$. Dimostrare che G è contenuto nel gruppo moltiplicativo $U(R[G])$ degli elementi invertibili di $R[G]$.

(c) Siano $f : R \to A$ un omomorfismo di anelli unitari e $h : G \to (A, \cdot)$ un omomorfismo di monoidi. Allora esiste un unico omomorfismo di anelli unitari $\rho : R[G] \to A$ tale che $\rho \circ \iota_R = f$ e $\rho \circ \iota_G = h$.

(d) Se H è un sottogruppo di G, allora esiste un unico omomorfismo di anelli unitari iniettivo $\rho : R[H] \to R[G]$ tale che $\rho \restriction_R = id_R$ e $\rho \restriction_H$ è l'inclusione di H in G.

(e) Dimostrare che l'anello gruppale $R[G]$ è determinato unicamente dalle proprietà (a), (b) e (c). In altre parole, se B è un anello commutativo unitario tale che esistono $j_R : R \to B$ omomorfismo iniettivo di anelli unitari e $j_G : G \to (B, \cdot)$ un omomorfismo iniettivo di monoidi tali che per ogni anello commutativo unitario A e per ogni $f : R \to A$ omomorfismo di anelli unitari e $h : G \to (A, \cdot)$ un omomorfismo di monoidi, esiste un unico omomorfismo di anelli unitari $\sigma : B \to A$ tale che $\sigma \circ j_R = f$ e $\sigma \circ j_G = h$, allora esiste un isomorfismo di anelli unitari da B a $R[G]$.

Esercizio 10.25 Sia R un anello commutativo unitario e siano G_1 e G_2 due gruppi finiti. Allora $R[G_1 \times G_2]$ è isomorfo a $(R[G_1])[G_2]$.

Esercizio 10.26 Sia G un gruppo con due elementi. Dimostrare che l'anello gruppale $\mathbb{R}[G]$ definito nell'esercizio 9.20 è isomorfo a $\mathbb{R} \times \mathbb{R}$.

Esercizio 10.27 Sia G un gruppo con tre elementi. Dimostrare che l'anello gruppale $\mathbb{R}[G]$ definito nell'esercizio 9.20 è isomorfo a $\mathbb{R} \times \mathbb{C}$.

Esercizio 10.28 Dato A un anello commutativo unitario, sia $e \in A$ diverso da $0, 1$ tale che $e^2 = e$. Allora gli ideali principali $A_1 = (e)$ e $A_2 = (1 - e)$, considerati come anelli, sono unitari e inoltre $A \cong A_1 \times A_2$.

Esercizio 10.29 Siano R un anello commutativo unitario in cui 2 è invertibile e $(G, \cdot)$ un gruppo ciclico di ordine 2. Dimostrare che l'anello gruppale $R[G]$ è isomorfo a $R \times R$.

Esercizio 10.30 Siano A_1, A_2 anelli commutativi unitari. Dimostrare che in $B = A_1 \times A_2$ esiste un idempotente j non banale, cioè $0_B \neq j \neq 1_B$.

Esercizio 10.31 Sia R un dominio tale che $R[G] \cong R_1 \times R_2$ dove $(G, \cdot)$ è un gruppo ciclico di ordine 2 e R_1 e R_2 sono anelli unitari. Dimostrare che 2 è invertibile in R.

Esercizio 10.32 Sia G il gruppo ciclico di ordine 2. Per un dominio R le seguente condizioni sono equivalenti:

(a) $R[G] \cong R \times R$;

(b) 2 è invertibile in R.

Esercizio 10.33 Un anello commutativo unitario si dice *Booleano* se $b^2 = b$ vale per ogni $b \in B$.

(a) Provare che la caratteristica di B è uguale a 2.
(b) Provare che B ha divisori dello zero qualora $|B| > 2$.
(c) Ogni ideale primo di B è massimale.
(d) Ogni ideale finitamente generato di B è principale.
(e) * Verificare che se B è finito, allora B è ismorfo all'anello $\mathbb{Z}_2^n$ per un opportuno $n \in \mathbb{N}$.

Esercizio 10.34 Dimostrare che se un elemento di un reticolo distributivo limitato ammette complemento, tale complemento è unico.

Esercizio 10.35 Sia X un insieme non vuoto. Allora l'insieme parzialmente ordinato $\mathcal{P}(X)$ di tutte le parti di X è un reticolo di Boole.

Esercizio 10.36 Dimostrare che l'insieme degli ideali $(\mathcal{J}(L), \leq)$ di un reticolo distributivo limitato L, come dalla definizione 10.30, contiene elementi massimali.

Esercizio 10.37 Sia $f : L \to L_1$ un omomorfismo di reticoli limitati. Dimostrare che l'insieme $I = \{x \in L : f(x) = 0\}$ è un ideale di L.

Esercizio 10.38 Individuare gli ideali primi del reticolo di tutti i divisori di 36 ordinato per divisibilità.

Esercizio 10.39 Un *filtro* su un insieme X è una famiglia $\mathcal{F}$ di sottoinsiemi di X con le seguenti proprietà:

(a) $\emptyset \notin \mathcal{F}$;
(b) se $A \in \mathcal{F}$ e $A \subseteq B \subseteq X$, allora anche $B \in \mathcal{F}$;
(c) se $A \in \mathcal{F}$ e $B \in \mathcal{F}$, allora anche $A \cap B \in \mathcal{F}$.

Poiché $\mathcal{F} \subseteq \mathcal{P}(X)$, l'insieme $F(X)$ dei filtri su X è un sottoinsieme di $\mathcal{P}(\mathcal{P}(X))$ ed è quindi ordinato con l'ordine indotto da $\mathcal{P}(\mathcal{P}(X))$, cioè diremo che $\mathcal{F} \leq \mathcal{G}$ per due filtri se $\mathcal{F} \subseteq \mathcal{G}$. Dimostrare che $F(X)$ ha elementi massimali[1].

Esercizio 10.40 Sia X un insieme infinito.

(a) Verificare che la famiglia $\mathfrak{F}_X$ di tutti i sottoinsiemi cofiniti di X, cioè con complemento finito è un filtro secondo la definizione data nell'esercizio 10.39, noto come il *filtro di Fréchet* su X.
(b) (Esercizio di analisi I) Verificare che una successione $\{x_n\}$ di numeri reali converge a $x \in \mathbb{R}$ se e solo se per ogni $\varepsilon > 0$ l'insieme $\{n \in \mathbb{N} : |x - x_n| < \varepsilon\}$ appartiene a $\mathfrak{F}_{\mathbb{N}}$.

---

[1] I filtri massimali si chiamano anche *ultrafiltri*. I filtri sono un mezzo fondamentale dell'*analisi* e della *topologia*.

Esercizio 10.41 Sia L un reticolo distributivo limitato. Un sottoinsieme F di L si dice un *filtro* se $0 \notin F$, $a \wedge b \in F$ per ogni $a, b \in F$ e se $a \in F$ e $a \leq x$ per qualche $x \in L$ implica $x \in F$. Dimostrare che:

(a) per ogni $a \in L$ l'insieme $\uparrow a = \{x \in L : x \geq a\}$ è un filtro;
(b) se L è finito, allora tutti i filtri di L sono della forma $\uparrow a$;
(c) se L è un reticolo di Boole, allora un sottoinsieme F di L è un filtro se e solo se l'insieme $I = \{\overline{x} : x \in F\}$ è un ideale di L, dove $\overline{x}$ è l'unico complemento di x in L.

Esercizio 10.42 Siano X un insieme, K un campo e A l'insieme K^X delle funzioni $X \to K$. Allora A è un anello commutativo unitario, con le operazioni definite nell'esercizio 9.4. Ponendo

$$Z(f) = \{x \in X : f(x) = 0\}$$

per $f \in A$, provare che:

(a) $f \in A$ è invertibile se e solo se $Z(f) = \emptyset$, quindi l'insieme $U(A)$ degli elementi invertibili di A coincide con l'insieme $(K \setminus \{0\})^X$ delle funzioni $X \to K \setminus \{0\}$, cioè delle funzioni $X \to K$ che non assumono il valore 0;
(b) se $|X| > 1$, allora ogni elemento non invertibile di A è divisore dello 0;
(c) per $f, g \in A$ risulta $Z(fg) = Z(f) \cup Z(g)$ e $Z(f+g) \supseteq Z(f) \cap Z(g)$;
(d) per $f, g \in A$, f divide g in A se e solo se $Z(f) \subseteq Z(g)$, in particolare f e g generano lo stesso ideale principale se e solo se $Z(f) = Z(g)$;
(e) $f \in A$ è idempotente, cioè $f = f^2$ se e solo se $f(x) = 1$ per ogni $x \in X \setminus Z(f)$, quindi ogni idempotente $f \in A$ è univocamente determinato dall'insieme $Z(f)$;
(f) ogni ideale principale è generato da un idempotente;
(g) ogni ideale finitamente generato di A è principale, in particolare se X è finito allora ogni ideale di A è principale;
(h) ogni ideale primo di A è massimale;
(i) per $x \in X$ l'insieme $M_x = \{f \in A : f(x) = 0\}$ è un ideale principale di A;
(j) per ogni $x \in X$ l'ideale M_x di A è massimale;
(k) ogni ideale massimale finitamente generato di A è di questo tipo, in particolare, se X è finito, allora ogni ideale massimale di A è di questo tipo;
(l*) mostrare con un esempio che, se X è infinito, esistono ideali massimali di A che non sono finitamente generati;
(m) se X e Y sono equipotenti, allora $K^X \cong K^Y$;
(n) se X è unione disgiunta di due suoi sottoinsiemi X_1 e X_2, allora

$$K^X \cong K^{X_1} \times K^{X_2}$$

come anelli;
(o) esiste un anello B tale che $B \cong B \times B$;
(p*) se X è infinito esiste una biezione tra gli ideali propri di A ed i filtri $\mathcal{F}$ di X.

Esercizio 10.43 Sia $\{K_i\}_{i \in I}$ una famiglia di campi. Riformulare e provare le proprietà (a)-(l) dell'esercizio 10.42 per l'anello $A = \prod_{i \in I} K_i$.

Esercizio 10.44 Nell'anello $A = \mathbb{Z}[\sqrt{2}]$ si considerino gli ideali $I = (2)$, $J = (3)$. Dire se gli anelli quozienti A/I e A/J sono campi.

Esercizio 10.45 Nell'anello $A = \mathbb{Z}[\sqrt{5}]$, sia $I = (5)$. Studiare l'anello quoziente A/I:

(a) provare che se $a \equiv 0 \bmod 5$, allora l'elemento $a + b\sqrt{5} + I$ è nilpotente;
(b) provare che se $a \not\equiv 0 \bmod 5$, allora l'elemento $a + b\sqrt{5} + I$ è invertibile;
(c) quali sono gli ideali di A/I?

Esercizio 10.46 Sia $A = \mathbb{Z}[\sqrt{5}]$. Per $\alpha = x + \sqrt{5}y \in A$ definiamo la norma di α con $N(\alpha) = x^2 - 5y^2$. Sia $M = \{\alpha \in A : N(\alpha) \text{ pari}\}$. Dire se M è ideale di A e, in caso affermativo, dire se M è massimale.

Esercizio 10.47 * Dimostrare che un anello commutativo unitario A è isomorfo ad un sottoanello di un anello regolare se e solo se A non ha elementi nilpotenti non nulli.

11

Anelli di polinomi

Lo scopo principale di questo capitolo è di introdurre l'anello di polinomi $A[x]$ sopra un anello unitario A e viene fatto nel primo paragrafo. Questa costruzione specifica per gli anelli è di grande importanza per le sue proprietà universali e anche per la teoria dei campi. Nel secondo paragrafo si studiano i domini fattoriali che soddisfano il teorema fondamentale dell'aritmetica, cioè i domini in cui ogni elemento non invertibile si fattorizza in modo unico in prodotto di elementi primi. Nel terzo paragrafo si dimostra che i domini principali, cioè i domini in cui ogni ideale è principale, hanno questa proprietà. Nel quarto paragrafo si studiano i domini euclidei, in cui vale una legge di divisione con resto, come in $\mathbb{Z}$. I domini euclidei risultano principali. Viene inoltre data la dimostrazione che l'anello degli interi di Gauss è un dominio euclideo. Nei paragrafi 1, 6 e 7 queste proprietà vengono studiate in un caso particolare molto rilevante, gli anelli di polinomi. Nel quinto paragrafo si studia la connessione tra divisibilità nell'anello dei polinomi e le radici di un polinomio, si dimostra il teorema di Ruffini.

11.1 L'anello dei polinomi $A[x]$

I polinomi sono conosciuti a tutti gli studenti fin dalle scuole superiori. Vedremo ora i polinomi sopra un anello di base A come elementi di un certo anello che risulterà avere proprietà molto buone, qualora l'anello A sia un campo.

Abbiamo già visto che per un anello commutativo unitario B, un elemento $b \in B$ e un sottoanello A di B, il sottoanello $A[b]$ di B generato da A e da b coincide con l'insieme di tutte le somme del tipo $a_0+a_1b+a_2b^2+\ldots+a_nb^n$, dove $a_0, \ldots, a_n \in A$ e $n \in \mathbb{N}$, come dimostrato nell'esercizio 9.14.

Nel seguito denoteremo con $A[b]$ il sottoanello descritto sopra e diremo che $A[b]$ è una *estensione semplice di A*.

Per esempio $\mathbb{C} = \mathbb{R}[i]$ è un'estensione semplice di $\mathbb{R}$. Come è noto vale $i^2 = -1$. In altre parole, due espressioni

$$a_0 + a_1i + a_2i^2 + \ldots a_ni^n \quad \text{e} \quad b_0 + b_1i + a_2i^2 + \ldots + b_mi^m$$

possono coincidere anche se non coincidono i rispettivi coefficienti $a_0, a_1, \ldots$ e $b_0, b_1, \ldots$. Raccogliendo tutti i termini a sinistra possiamo anche dire che esiste una espressione

$$c_0 + c_1 i + \ldots + c_s i^s = 0$$

nella quale non tutti i coefficienti $c_0, c_1, \ldots c_s$ sono nulli: ad esempio $1 + i^2 = 0$.

In generale diremo che un'estensione semplice $A[x]$ è *anello di polinomi di x sopra A* se non esistono elementi $a_0, a_1, \ldots, a_n$ di A, non tutti nulli, tali che

$$a_0 + a_1 x + \ldots + a_n x^n = 0.$$

In altre parole, se due espressioni

$$a_0 + a_1 x + \ldots + a_n x^n \quad \text{e} \quad b_0 + b_1 x + \ldots + b_m x^m$$

coincidono, allora

$$n = m \quad \text{e} \quad a_0 = b_0, \ldots, a_n = b_n.$$

Una tale espressione $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ si dice *polinomio in x a coefficienti in A*.

L'estensione semplice $A[x]$ è stata definita nell'ambito di un anello B che contiene x e A come sottoanello. Dimostriamo ora esplicitamente che esiste l'anello dei polinomi $A[x]$ su un anello commutativo unitario A senza far ricorso ad un simile anello B, cioè costruiremo $A[x]$ a partire solo da A e x.

Lemma 11.1. *Sia A un anello commutativo unitario. Allora esiste l'anello dei polinomi $A[x]$ sopra A.*

DIMOSTRAZIONE. Consideriamo l'insieme S di tutte le successioni infinite

$$(a_0, a_1, \ldots)$$

di elementi di A tali che esiste $n_0 \in \mathbb{N}$ con $a_n = 0$ per ogni $n \geq n_0$. S è un sottoinsieme del prodotto cartesiano $A^{\mathbb{N}}$. Vogliamo ora definire due operazioni in S. Definiamo la somma di due successioni di questo tipo componente per componente

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots).$$

Il prodotto è definito da

$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (c_0, c_1, \ldots), \text{ dove } c_i = \sum_{j+k=i} a_j b_k.$$

Non è difficile vedere che se $a_n = 0$ per tutti gli $n > n_0$ e se $b_m = 0$ per tutti gli $m > m_0$, allora $c_i = 0$ per tutti gli $i > n_0 + m_0$, pertanto la successione $(c_0, c_1, \ldots)$ appartiene a S. È una facile verifica mostrare che l'insieme S con queste due operazioni risulta essere un anello commutativo unitario, con unità $1_S = (1, 0, 0, 0, \ldots)$. Inoltre gli elementi del tipo $(a, 0, 0, 0, \ldots)$, $a \in A$, formano un sottoanello A_1 di S isomorfo all'anello A. L'elemento $x = (0, 1, 0, 0, 0, \ldots)$ di S soddisfa

$$x^n = (\underbrace{0, \ldots, 0}_{n \text{ volte}}, 1, 0, 0, 0, \ldots),$$

quindi ogni elemento $(a_0, a_1, \ldots)$ di S con $a_n = 0$ per tutti gli $n > n_0$ si può scrivere come somma

$$a_0 1_S + a_1 x + \ldots + a_{n_0} x^{n_0} \tag{1}$$

Questo dimostra che $S = A[x]$, identificando A con A_1. Per vedere che questo è un anello di polinomi basta notare che un'espressione del tipo (1) risulta essere 0 se e solo se tutti gli a_i sono nulli. □

Per dimostrare l'unicità dell'anello dei polinomi, a meno di isomorfismi, dimostriamo dapprima un teorema che vale per ogni estensione semplice di un anello commutativo unitario. Il teorema 11.2 garantisce che l'anello dei polinomi su un anello commutativo unitario A è in un certo senso l'estensione semplice "universale", cioè ogni estensione semplice di A è isomorfa ad un quoziente dell'anello dei polinomi $A[x]$.

Teorema 11.2. *Sia* $B = A[b]$ *un'estensione semplice di* A*, anello commutativo unitario e sia* $A[x]$ *un anello di polinomi di* x *su* A*. Allora:*

(a) esiste un unico omomorfismo di anelli unitari $f : A[x] \to B$ *tale che* $f(a) = a$ *per ogni* $a \in A$ *e* $f(x) = b$*;*
(b) B *è isomorfo ad un quoziente dell'anello* $A[x]$.

DIMOSTRAZIONE. (a) La posizione $f(a) = a$ per ogni $a \in A$ e $f(x) = b$ determina anche il valore di f su un polinomio arbitrario di $A[x]$. Si verifica immediatamente che f è un omomorfismo di anelli unitari.

(b) Basta notare che l'omomorfismo del punto (a) è suriettivo e applicare il primo teorema di omomorfismo 10.4. □

Dal teorema 11.2 segue che l'anello di polinomi $A[x]$ sopra A è unico a meno di isomorfismi che fissano gli elementi di A.

Corollario 11.3. *L'anello di polinomi* $A[x]$ *sopra* A *è unico, a meno di isomorfismi che fissano gli elementi di* A.

DIMOSTRAZIONE. Sia $A[y]$ un anello di polinomi di su A; allora per il teorema 11.2 esiste un omomorfismo di anelli unitari $f : A[x] \to A[y]$ tale che $f(a) = a$ per ogni $a \in A$ e $f(x) = y$. Analogamente esiste un omomorfismo di anelli unitari $g : A[y] \to A[x]$ tale che $g(a) = a$ per ogni $a \in A$ e $g(y) = x$. La composizione $g \circ f : A[x] \to A[x]$ è l'omomorfismo identico e lo stesso vale per la composizione $f \circ g : A[y] \to A[y]$. Di conseguenza f e g sono isomorfismi. □

Sia A un anello commutativo unitario. Nel seguito denoteremo con $A[x]$ l'anello dei polinomi di x sopra A. Abbiamo appena visto che tale anello è unico a meno di isomorfismi che lasciano fissi gli elementi di A.

Diamo ora alcune definizioni.

Definizione 11.4. Il polinomio che corrisponde alla successione costante 0, cioè $a_n = 0$ per tutti gli $n \in \mathbb{N}$ si dice *polinomio nullo.*

Nel seguito scriveremo un polinomio non nullo dato da (1) come

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n, \quad \text{con } a_n \neq 0.$$

Definizione 11.5. Se $f(x) = a_0 + a_1 x + \ldots + a_n x^n \neq 0$ e $a_n \neq 0$, l'intero n si chiama il *grado* di $f(x)$ e si denota con $\deg f$. Il coefficiente a_n si dice *coefficiente direttivo.* Infine il polinomio $f(x)$ si dice *monico* se $a_n = 1$.

Al polinomio nullo non si attribuisce un grado. Un polinomio non nullo si dice una *costante* se il suo grado è 0. Proviamo alcuni lemmi che riguardano il grado del prodotto di due polinomi e che saranno utili in seguito.

Lemma 11.6. *Sia A un dominio. Se $f(x)$ e $g(x)$ sono due elementi non nulli di $A[x]$, allora*

$$\deg fg = \deg f + \deg g.$$

DIMOSTRAZIONE. Siano

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \quad \text{e} \quad g(x) = b_0 + b_1 x + \ldots + b_m x^m,$$

con $a_n \neq 0 \neq b_m$. Allora $\deg f = n$ e $\deg g = m$. Dalla definizione di prodotto otteniamo

$$f(x)g(x) = c_0 + c_1 x + \ldots + c_{n+m} x^{n+m},$$

ove $c_{n+m} = a_n b_m \neq 0$, perché A è un dominio. Pertanto $\deg fg = n + m$. □

Osserviamo che nel lemma 11.6 l'ipotesi che A sia un dominio si è rivelata essenziale: nell'anello $\mathbb{Z}_4[x]$ il polinomio $f(x) = 2x + 1$ ha grado 1, mentre $f(x) \cdot f(x) = 1$ ha grado 0. Vediamo due corollari.

Corollario 11.7. *Se A è un dominio e $f(x)$, $g(x)$ sono due polinomi non nulli di $A[x]$, allora* $\deg f \leq \deg fg$.

Corollario 11.8. *Se A è un dominio, allora anche $A[x]$ è un dominio.*

DIMOSTRAZIONE. Se $f(x)$ e $g(x)$ sono due elementi non nulli di $A[x]$ e

$$h(x) = f(x)g(x),$$

allora $\deg h = \deg f + \deg g$ per il lemma 11.6 e pertanto $h(x)$ non può essere il polinomio nullo. □

Segue una proprietà molto importante dell'anello dei polinomi.

Lemma 11.9. (Algoritmo della divisione) *Siano $f(x)$ e $g(x)$ due polinomi di $A[x]$, ove A è un anello commutativo unitario e il coefficiente direttivo di $g(x)$ sia invertibile. Allora esistono due polinomi $q(x)$ ed $r(x)$ tali che $f(x) = q(x)g(x) + r(x)$, con $r(x) = 0$ oppure* $\deg r < \deg g$.

DIMOSTRAZIONE. Se $f = 0$ poniamo $q = r = 0$. Altrimenti possiamo scrivere

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \quad \text{e} \quad g(x) = b_0 + b_1x + \ldots + b_mx^m,$$

con $a_n \neq 0 \neq b_m$ e b_m invertibile, da cui $n = \deg f$ e $m = \deg g$. Se $n < m$, basta prendere $q(x) = 0$ e $r(x) = f(x)$. Dimostriamo il lemma per induzione su n. Se $n = 0$ abbiamo due casi. Il caso $m > n = 0$, l'abbiamo già considerato. Se $m = 0$, si ha $f(x) = a_0$ e $g(x) = b_0 \neq 0$, b_0 invertibile. Allora poniamo $q(x) = a_0b_0^{-1}$ e $r(x) = 0$. Supponiamo ora $n \geq 1$, $n \geq m$ e che l'asserto sia vero per tutti i numeri naturali $k < n$. Sia

$$f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x),$$

allora $\deg f_1 \leq n-1$. Applichiamo l'ipotesi induttiva ad f_1 e troviamo due polinomi $q_1(x)$ ed $r(x)$, tali che

$$f_1(x) = q_1(x)g(x) + r(x) \quad \text{con } r(x) = 0 \text{ oppure } \deg r < \deg g.$$

Allora

$$f(x) = f_1(x) + a_nb_m^{-1}x^{n-m}g(x) = q_1(x)g(x) + r(x) + a_nb_m^{-1}x^{n-m}g(x) =$$

$$= (q_1(x) + a_nb_m^{-1}x^{n-m})g(x) + r(x),$$

da cui la conclusione, ponendo $q(x) = q_1(x) + a_nb_m^{-1}x^{n-m}$. □

Il campo dei quozienti dell'anello dei polinomi $K[x]$ sopra un campo K si dice anche *campo delle funzioni razionali* sopra K e si denota con $K(x)$. Un tipico elemento di $K(x)$ è una frazione $\frac{f(x)}{g(x)}$, dove $f(x)$ e $g(x)$ sono polinomi di x e $g(x) \neq 0$.

11.2 Domini fattoriali

Sia A un dominio di integrità. Per $a \in A^*$ e $b \in A$ diremo che *a divide b*, scrivendo $a|b$, se esiste $c \in A$ tale che $b = ac$. In tal caso diremo che *a è divisore di b*. Si ha $a|0$ per ogni $a \in A^*$. Questo definisce una relazione binaria $a|b$, "a divide b", in A^*.

Definizione 11.10. Se $a|b$ e $b|a$ diremo che *a è associato* a b e lo denoteremo con $a \sim b$.

È facile vedere che $\sim$ è una relazione di equivalenza in A^*. L'insieme $U(A)$ degli elementi invertibili di A coincide con la classe di equivalenza di 1. Più in generale la classe di equivalenza di $a \in A^*$ coincide con l'insieme $aU(A) = \{ac : c \in U(A)\}$, cioè $b \sim a$ se e solo se $b = ac$ con $c \in U(A)$. Chiaramente ogni $b \in A^*$ ha come divisori tutti gli elementi invertibili ed anche tutti gli a tali che $a \sim b$. Questi sono i *divisori impropri* di b. Un divisore non improprio di b si dice *divisore proprio* di b.

Dimostriamo un semplicissimo lemma che collega la divisibilità con l'ordine per inclusione tra gli ideali principali.

Lemma 11.11. *Siano a, b elementi non nulli di un anello commutativo unitario A. Allora a divide b se e solo se $(b) \subseteq (a)$. Inoltre $(a) = (b)$ se e solo se a e b sono associati.*

DIMOSTRAZIONE. Per definizione a divide b se e solo se $b = ac$ per qualche $c \in A$. Questo accade se e solo se $b \in (a)$, ciò è equivalente a dire che $(b) \subseteq (a)$. Il secondo enunciato segue dal primo e dalla definizione di elementi associati. □

Definizione 11.12. Un elemento $b \in A^*$ si dice *irriducibile* se non è invertibile e non ha divisori propri.

Un elemento $c \in A^*$ si dice *primo* se c non è invertibile e se $c|ba$ per qualche $a, b \in A$ implica $c|a$ oppure $c|b$.

Lemma 11.13. *In un dominio A ogni elemento primo è irriducibile.*

DIMOSTRAZIONE. Sia p un elemento primo del dominio A. Se p non fosse irriducibile, esisterebbero dei divisori propri a e b di p con $p = ab$. In tal caso p non dividerebbe né a né b, ma $p|ab$, in contraddizione con la definizione di primo. □

Introduciamo una classe di domini dove gli elementi irriducibili servono da "atomi" con i quali si possono ottenere, in modo unico, tutti gli altri elementi di A tramite moltiplicazioni. Qui l'unicità si intende nel modo seguente. Se $a = p_1 \dots p_n = q_1 \dots q_s$ sono due fattorizzazioni di a in prodotto di elementi irriducibili, allora $n = s$ e dopo opportuna permutazione dei fattori, si ha

$$q_1 \sim p_1, \dots, q_s \sim p_n.$$

Definizione 11.14. Il dominio A si dice *dominio fattoriale* se tutti gli elementi non invertibili di A^* hanno una fattorizzazione unica in prodotto di elementi irriducibili.

Proviamo ora che nel caso dei domini fattoriali vale anche il viceversa dell'enunciato del lemma 11.13.

Lemma 11.15. *In un dominio fattoriale A ogni elemento irriducibile è primo.*

DIMOSTRAZIONE. Sia c un elemento irriducibile di A; allora c non è invertibile. Supponiamo che c divida ab. Se a è invertibile, c divide $a^{-1}ab = b$ e possiamo concludere. Analogamente se b è invertibile. Possiamo supporre che né a né b siano invertibili. Allora a e b hanno una fattorizzazione unica come prodotto di elementi irriducibili, cioè esistono elementi irriducibili $p_1, \dots, p_r, q_1, \dots q_s$ tali che $a = p_1 \dots p_r$ e $b = q_1 \dots q_s$. Dal fatto che c divide $ab = p_1 \dots p_r q_1 \dots q_s$ e che c è irriducibile, otteniamo per l'unicità della decomposizione che $c \sim p_i$ per qualche $i = 1, \dots, r$ oppure $c \sim q_j$ per qualche $j = 1, \dots, s$. Di conseguenza $c|a$ oppure $c|b$. □

Quindi nei domini fattoriali un elemento è primo se e solo se è irriducibile. Vediamo il ruolo di questa proprietà per quanto riguarda l'unicità della fattorizzazione.

Lemma 11.16. *Sia A un dominio in cui ogni elemento irriducibile sia primo. Se ogni elemento non invertibile di A^* si fattorizza in prodotto di irriducibili, allora tale fattorizzazione è unica.*

DIMOSTRAZIONE. Sia $a \in A$ e supponiamo che $a = p_1 \dots p_n = q_1 \dots q_s$ siano due fattorizzazioni di a in prodotto di elementi irriducibili e quindi primi. Ragioniamo per induzione su n. Se $n = 1$, avremo $p_1 = q_1 \dots q_s$, che implica $s = 1$ poiché p_1 è irriducibile. Supponiamo adesso $n > 1$. Allora p_1 divide il prodotto $q_1 \dots q_s$ e poiché p_1 è primo, divide uno dei fattori, diciamo q_1. Poiché q_1 è irriducibile, concludiamo che $q_1 \sim p_1$. Dopo la cancellazione, abbiamo $p_2 \dots p_n \sim q_2 \dots q_s$. Poiché l'elemento $a' = p_2 \dots p_n$ è prodotto di un numero minore di n elementi primi, per l'ipotesi induttiva la sua fattorizzazione deve essere unica a meno di permutazione dei fattori, cioè si può supporre $s = n$ e $q_2 \sim p_2, \dots, q_s \sim p_n$. □

La proprietà successiva dei domini fattoriali riguarda le catene crescenti di ideali principali.

Lemma 11.17. *Sia A un dominio fattoriale. Allora ogni catena crescente di ideali principali di A*

$$(a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots \tag{2}$$

si stabilizza, cioè esiste $n_0 \in \mathbb{N}$ tale che $(a_n) = (a_{n_0})$ per tutti gli $n \geq n_0$.

DIMOSTRAZIONE. Per il lemma 11.11 ogni a_n è un divisore proprio di a_{n-1}. Se

$$a_1 = p_1 \dots p_m,$$

chiaramente ogni catena di divisori propri di a_1 del tipo

$$a_2 | a_1, \ a_3 | a_2, \ \dots, \ a_n | a_{n-1}, \ \dots$$

non può avere lunghezza maggiore di m. Infatti, se a_2 è divisore proprio di a_1, allora si deduce facilmente dall'unicità della fattorizzazione che ogni fattorizzazione di a_2 in prodotto di elementi irriducibili deve avere meno di m fattori. Pertanto $(a_n) = (a_{m+1})$ per ogni $n \geq m + 1$. □

Osservazione 11.18. Nel seguito avremo bisogno di una proprietà equivalente a quella considerata nel lemma precedente. Per comodità la formuliamo in generale. Se in un anello commutativo A ogni catena crescente di ideali principali si stabilizza, allora ogni famiglia non vuota $\mathcal{I}$ di ideali principali di A ha un elemento massimale rispetto all'inclusione. Infatti si può dimostrare la seguente proprietà più forte: ogni elemento (a) di $\mathcal{I}$ è contenuto in un elemento massimale (m) di $\mathcal{I}$. Supponiamo per assurdo che questo non sia vero per un certo $(a) \in \mathcal{I}$. Allora esisterebbe una catena propriamente crescente (2) di elementi di $\mathcal{I}$ con $(a_1) = (a)$, assurdo.

Ora siamo in grado di dimostrare il teorema principale sui domini fattoriali. Abbiamo verificato nei lemmi 11.15 e 11.17 che negli anelli fattoriali gli elementi irriducibili sono primi e ogni catena crescente di ideale principali di A si stabilizza.

Ora dimostriamo che queste due proprietà caratterizzano i domini fattoriali.

Teorema 11.19. *Un dominio A è fattoriale se e solo se gli elementi irriducibili di A sono primi e ogni catena crescente di ideale principali di A si stabilizza.*

DIMOSTRAZIONE. Abbiamo già verificato la necessità di queste due condizioni nei lemmi 11.15 e 11.17.

Supponiamo che gli elementi irriducibili di A siano primi e ogni catena crescente di ideale principali di A si stabilizzi. Per dimostrare che A è un dominio fattoriale dobbiamo verificare in primo luogo che ogni elemento non invertibile di A è prodotto di elementi irriducibili di A. A questo scopo consideriamo l'insieme $\mathcal{S}$ di tutti gli elementi non nulli e non invertibili di A che non si possono presentare come prodotto di elementi irriducibili di A. Supponiamo per assurdo che $\mathcal{S}$ non sia vuoto e consideriamo la famiglia non vuota $\mathcal{I} = \{(a) : a \in \mathcal{S}\}$ di ideali di A. Per l'ipotesi e l'osservazione 11.18 l'insieme ordinato $(\mathcal{I}, \subseteq)$ ha un elemento massimale (m). Poiché $m \in \mathcal{S}$, $m \neq 0$ non è irriducibile, quindi esistono elementi non invertibili $a, b \in A$ tali che $m = ab$. Pertanto sia (a) che (b) contengono propriamente (m) per il lemma 11.11. Allora $(a) \notin \mathcal{I}$ e $(b) \notin \mathcal{I}$. Di conseguenza $a \notin \mathcal{S}$ e $b \notin \mathcal{S}$ sono prodotto di elementi irriducibili, dunque lo è anche m, contraddicendo il fatto che $m \in \mathcal{S}$. Questa contraddizione conclude la dimostrazione del fatto che ogni elemento non invertibile di A è prodotto di irriducibili di A.

Dall'ipotesi che ogni irriducibile è primo, segue l'unicità della fattorizzazione, applicando il lemma 11.16. □

Sia A un dominio fattoriale. Per ogni elemento irriducibile $p \in A$ scegliamo un elemento della classe $[p]_\sim$ di tutti gli elementi associati a p e fissiamo in questo modo un insieme di rappresentanti $P(A)$ per tutte le classi $[p]_\sim$. Per esempio, come $P(\mathbb{Z})$ possiamo prendere sia l'insieme dei numeri primi positivi, sia l'insieme dei numeri primi negativi. Mentre per un campo arbitrario K, come $P(K[x])$ possiamo prendere l'insieme dei polinomi irriducibili monici, si veda il paragarafo 11.6.

Dopo aver fissato $P(A)$ come sopra, ogni elemento non nullo e non invertibile a di A si può scrivere in modo unico come prodotto $a = up_1^{n_1} \dots p_s^{n_s}$, dove u è un elemento invertibile, $n_1, n_2, \dots, n_s \in \mathbb{N}_+$ e $p_1, p_2, \dots, p_s \in P(A)$ sono a due a due distinti. Infatti una tale fattorizzazione si può ricavare immediatamente dall'esistenza della fattorizzazione in A e dalla scelta di $P(A)$. Supponiamo ora che

$$up_1^{n_1} \dots p_s^{n_s} = u'q_1^{m_1} \dots q_s^{m_t},$$

con $m_1, m_2, \dots, m_t \in \mathbb{N}_+$ e $q_1, q_2, \dots, q_t \in P(A)$ a due a due distinti. Allora per l'unicità della fattorizzazione possiamo dedurre che $t = s$ e dopo un'opportuna permutazione degli indici si può supporre $q_i = p_i$ per $i = 1, 2, \dots, s$. Sempre per l'unicità della fattorizzazione si ha anche $m_i = n_i$ per $i = 1, 2, \dots, s$. Questo implica anche $u' = u$ dopo le cancellazioni.

Osservazione 11.20. La presentazione $a = up_1^{n_1} \dots p_s^{n_s}$ ottenuta sopra permette di decidere facilmente se $a|b$, se uno conosce anche la fattorizzazione $b = u'q_1^{m_1} \dots q_t^{m_s}$ di b. Infatti $a|b$ se e solo se $s \leq t$ e dopo un'opportuna permutazione degli indici si ha $q_i = p_i$ e $n_i \leq m_i$ per $i = 1, 2, \dots, s$. Nel seguito supporremo $n_i, m_i \geq 0$ (cioè possono assumere anche il valore 0) allo scopo di poter scrivere sempre a e b come prodotti.

$$a = uq_1^{n_1} \dots q_s^{n_t} \quad \text{e} \quad b = u'q_1^{m_1} \dots q_s^{m_t}$$

con $u, u' \in U(A)$ e *gli stessi* $q_1, q_2, \ldots, q_t \in P(A)$. Per esempio, se un certo q_i non divide a, scriveremo $n_i = 0$ nella formula $a = uq_1^{n_1} \ldots q_s^{n_t}$.

Diamo ora un'altra nozione nota nell'anello degli interi, ma che può essere estesa in generale a qualsiasi dominio.

Definizione 11.21. Siano a, b elementi non nulli di un dominio A. Allora un elemento $d \in A$ si dice *massimo comun divisore (MCD)* di a e b se:

(1) $d|a$ e $d|b$;
(2) se $c|a$ e $c|b$, allora $c|d$.

Useremo la notazione $d = (a, b)$ per indicare che d è un massimo comun divisore di a e b. Osserviamo che se d e d' sono due massimi comuni divisori di a e b, allora per definizione $d|d'$ e $d'|d$, da cui segue che d e d' sono associati. È chiaro quindi che (a, b) è determinato a meno di un multiplo invertibile.

Definizione 11.22. Siano a, b elementi non nulli di un anello A. Allora a e b si dicono *coprimi* se $(a, b) = 1$.

Il lemma 11.11 permette di dare la seguente caratterizzazione del massimo comun divisore d di due elementi a, b di un dominio A: *l'ideale principale* (d) *contiene l'ideale* $(a) + (b)$ *ed è il più piccolo ideale principale con questa proprietà.* Vedremo nel lemma 11.24 come questa proprietà possa aiutare a descrivere meglio il massimo comun divisore.

Lemma 11.23. *In un dominio fattoriale ogni coppia di elementi non nulli ha massimo comun divisore.*

DIMOSTRAZIONE. Sia A un dominio fattoriale e siano a e b due elementi non nulli di A. Se a o b è invertibile, allora $(a, b) = 1$. Supponiamo pertanto a e b non invertibili e scriviamo le fattorizzazioni $a = p_1^{m_1} \ldots p_t^{m_t}$ e $b = p_1^{n_1} \ldots p_t^{n_t}$ di a e b come nell'osservazione 11.20, con $p_i \in P(A)$, e dove $m_1, n_1, \ldots, m_s, n_s$ possono essere eventualmente nulli. Allora segue dall'osservazione 11.20 che un comune divisore di a e b è $d = p_1^{l_1} \ldots p_s^{l_s}$, dove $l_i = \min\{m_i, n_i\}$ per $i = 1, \ldots, s$. Per vedere che d è un massimo comune divisore di a e b consideriamo un altro comune divisore

$$d' = vp_1^{k_1} \ldots p_t^{k_t}$$

di a e b, dove $v \in U(A)$. Allora $d'|a$ e $d'|b$ implicano $k_i \leq \min\{m_i, n_i\}$ per $i = 1, \ldots, t$. Quindi $d'|d$. Questo dimostra che $d = (a, b)$. □

11.3 Domini principali

Ricordiamo che un dominio di integrità A si dice principale se tutti gli ideali di A sono principali, come dalla definizione 9.20. Usando il teorema 11.19 dimostreremo che ogni dominio principale è fattoriale. A questo scopo avremo bisogno dei seguenti lemmi.

Lemma 11.24. *Siano A un dominio principale e $a, b \in A^*$. Allora esiste un massimo comun divisore d di a e b. Inoltre d è combinazione lineare di a e b.*

DIMOSTRAZIONE. Sia d il generatore dell'ideale principale $(a) + (b)$. Allora

$$(a) \subseteq (d) \quad \text{e} \quad (b) \subseteq (d) \implies d|a \text{ e } d|b.$$

Poiché $d \in (a) + (b)$, d è combinazione lineare di a e b, cioè esistono $l, m \in A$ tali che $d = la + mb$. Quindi se c divide a e b, c divide anche $la + mb = d$; ciò prova che d è un massimo comun divisore di a e b. □

Questa proprietà dei domini principali è più forte di quella vista nel lemma 11.23, per il fatto che d è combinazione lineare di a e b. Infatti, se si considera ad esempio l'anello dei polinomi $A = B[y]$, ove B è l'anello dei polinomi $B = \mathbb{R}[x]$, allora A è un dominio fattoriale per il teorema 11.56 e il massimo comun divisore di x ed y è 1, ma 1 non si può scrivere come combinazione lineare di x ed y.

Corollario 11.25. *Siano A un dominio principale e p un elemento irriducibile di A. Se p non divide un elemento $a \in A$, allora p ed a sono coprimi.*

DIMOSTRAZIONE. Per il lemma 11.24 esiste un massimo comun divisore $d = (p, a)$. Poiché $d|p$ e p è irriducibile, avremo che d è invertibile e quindi $d \sim 1$, da cui segue $(p, a) = 1$. □

Lemma 11.26. *Siano A un dominio principale e $a, b, c \in A^*$. Se c ed a sono coprimi e $c|ab$, allora $c|b$.*

DIMOSTRAZIONE. Essendo $1 = (a, c)$, per il lemma 11.24 possiamo scrivere

$$1 = ua + vc$$

con opportuni $u, v \in A$. Moltiplicando per b si trova $b = uab + vcb$. Poiché $c|ab$ e $c|c$, concludiamo che c divide b. □

Abbiamo visto che in un dominio fattoriale i concetti "irriducibile" e "primo" coincidono. Ciò avviene anche in un dominio principale.

Lemma 11.27. *Sia A un dominio principale. Allora ogni elemento irriducibile di A è primo.*

DIMOSTRAZIONE. Sia p un elemento irriducibile di A e supponiamo che p divida ab. Se p non divide a, allora p ed a sono coprimi per il corollario 11.25. Quindi, per il lemma 11.26, $p|ab$ implica $p|b$. Questo dimostra che p è primo. □

Teorema 11.28. *Ogni dominio principale è fattoriale.*

DIMOSTRAZIONE. Sia A un dominio principale. Dimostriamo prima che ogni catena crescente di ideale principali di A si stabilizza. Supponiamo di avere una catena crescente di ideali principali

$$(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_n) \subseteq \ldots.$$

L'unione I della catena è un ideale di A. Poiché A è un dominio principale, esiste un elemento $a \in I$ tale che $I = (a)$. Esiste n_0 tale che $a \in (a_{n_0})$. Allora $I = (a_{n_0})$, essendo $(a_{n_0}) \subseteq I$ e $(a_{n_0}) \subseteq (a) = I$. Pertanto $(a_n) = (a_{n_0})$ per tutti gli $n \geq n_0$.

Per dimostrare che A è fattoriale basta applicare il teorema 11.19 in virtù del lemma 11.27. □

Vediamo ora un'altra importante proprietà degli ideali di anelli principali. Avremo bisogno del seguente lemma più generale.

Lemma 11.29. *L'ideale (a) di un dominio A è un ideale primo se e solo se a è un elemento primo di A.*

DIMOSTRAZIONE. Vediamo che a non è primo se e solo se (a) non è primo. Infatti, a non è primo se e solo se esistono $b, c \in A$ tali che $a|bc$, ma a non divide b e a non divide c. Questo è equivalente a dire che esistono b, c tali che $b \notin (a)$ e $c \notin (a)$, ma $bc \in (a)$, cioè l'ideale principale (a) non è primo. □

Proposizione 11.30. *L'ideale (a) è un ideale massimale del dominio principale A se e solo se a è un elemento primo di A.*

DIMOSTRAZIONE. Supponiamo che a non sia primo. Allora per il lemma 11.29 l'ideale (a) non è primo e quindi non è nemmeno massimale.

Supponiamo viceversa che a sia primo e che $(a) \subseteq I \subseteq A$, dove I è un ideale di A con $(a) \neq I$. Per ipotesi esiste $i \in A$ tale che $I = (i)$ e quindi $a = ix$ per qualche $x \in A$. Allora a non divide i essendo $(a) \neq I$. Poiché a è irriducibile, essendo primo, concludiamo che i è invertibile e dunque $I = A$ per il lemma 9.21. □

Abbiamo visto che ci sono infiniti numeri primi. Dimostriamo ora che questa proprietà si estende a tutti domini principali (necessariamente infiniti) che non sono campi. Nel seguente teorema proviamo che se il numero degli elementi invertibili è finito, allora esistono infiniti elementi irriducibili.

Teorema 11.31. *Sia A un dominio principale infinito. Se $U(A)$ finito, allora A ha infiniti elementi irriducibili a due a due non associati.*

DIMOSTRAZIONE. Notiamo che A non è un campo essendo $U(A)$ finito.

Per la proposizione 11.30 un elemento p di A è irriducibile se e solo se l'ideale (p) è massimale. Poiché $p \sim p'$ se e solo se $(p) = (p')$, basta dimostrare che esistono infiniti ideali massimali distinti di A. Ragionando per assurdo supponiamo che $\{(p_1), (p_2), \ldots, (p_n)\}$ siano gli unici ideali massimali non nulli di A. Poiché A non è un campo, questo insieme non è vuoto. L'elemento $a = p_1 p_2 \ldots p_n$ è non nullo in quanto A è un dominio. Quindi l'ideale principale $I = (a)$ è infinito, poiché

$|I| = |A|$. Si ha $M \supseteq I$ per ogni ideale massimale M di A. Quindi per ogni elemento $x \in 1 + I$ abbiamo $x \notin M$ in quanto $x \in M$ e $x - 1 \in I \subseteq M$ implicano $1 \in M$, assurdo. Non essendo contenuto in alcun ideale massimale, l'elemento x risulta invertibile. Questo dimostra che $1 + I \subseteq U(A)$, pertanto $U(A)$ è infinito, assurdo. □

È molto più facile vedere che un dominio principale A con $U(A)$ infinito ha ugualmente infiniti elementi irriducibili distinti, se A non è un campo. Infatti poiché A non è un campo, esiste almeno un elemento irriducibile p di A. Ora gli elementi up, $u \in U(A)$, sono irriducibili e distinti. Tuttavia gli elementi irriducibili trovati in questo modo sono a due a due associati. Esistono domini principali A (necessariamente con $U(A)$ infinito) con un elemento irriducibile p, tale che ogni altro elemento irriducibile di A è associato a p, per esempio il dominio considerato nell'esercizio 9.49.

Esempio 11.32. Sia K un campo. Vediamo che l'anello dei polinomi $A = K[x]$ ha sempre infiniti polinomi irriducibili a due a due non associati. Quando K è infinito basta prendere infiniti elementi a due a due distinti a_n, $n \in \mathbb{N}$, di K e considerare i polinomi $x - a_n$.

Consideriamo ora un altro argomento, che funziona anche nel caso di campo finito K. Supponiamo per assurdo che $p_1(x), p_2(x), \ldots, p_n(x) \in A$ siano tutti i polinomi irriducibili a due a due non associati di A. Allora consideriamo il polinomio $f(x) = p_1(x)p_2(x)\ldots p_n(x) + 1$. Avendo grado maggiore dei gradi di ciascuno dei polinomi $p_i(x)$ non può essere associato a nessuno di essi. Quindi $f(x)$ non è irriducibile. Non essendo nemmeno invertibile, esiste un polinomio irriducibile $q(x)$ che divide $f(x)$. Allora $q(x)$ non può dividere nessuno dei polinomi $p_i(x)$, pertanto $q(x)$ non è associato a nessuno dei polinomi $p_i(x)$, assurdo.

11.4 Domini euclidei

Vedremo che una condizione sufficiente per avere a disposizione la fattorizzazione unica in prodotto di elementi irriducibili è la presenza di una funzione che "misura" la divisibilità e permette di eseguire "divisioni con resto" nel modo seguente.

Definizione 11.33. Il dominio A si dice *dominio euclideo* se ammette una funzione $\delta : A^* \to \mathbb{N}$, detta *norma*, con le seguenti proprietà:

(1) $\delta(ab) \geq \delta(a)$ per tutti gli elementi non nulli a, b di A;
(2) se a e $b \neq 0$ sono elementi di A, possiamo trovare $q, r \in A$ tali che $a = qb + r$ e $r = 0$ oppure $\delta(r) < \delta(b)$.

La presenza di una norma che definisce i domini euclidei è abbastanza naturale, come mostrano i seguente esempi.

Esempio 11.34. (a) Il dominio $\mathbb{Z}$ con la norma $\delta : \mathbb{Z} \to \mathbb{N}$ definita con $\delta(a) = |a|$ risulta un dominio euclideo, si veda il teorema 3.6.

(b) Sia A un campo. Allora per $a, b \in A^*$ vale sempre sia $a|b$ sia $b|a$. Allora A risulta un dominio euclideo con δ una qualsiasi funzione costante $A^* \to \mathbb{N}$.

(c) I domini con la proprietà del punto (b) sono esattamente i campi. In altre parole, se A è un dominio euclideo con δ costante, allora A è un campo. Infatti, nella parte (2) della definizione 11.33 si può avere solo il caso $r = 0$ perché δ è costante. Ma questo significa che ogni elemento $b \neq 0$ divide 1, cioè b è invertibile.

Si veda anche il teorema 11.48 per un altro esempio importante di dominio euclideo.

Osservazione 11.35. Sia A un dominio euclideo con norma δ. Dai valori di δ si possono ricavare diverse informazioni. Poniamo $m = \delta(1)$, allora dalla parte (1) della definizione 11.33 che

(a) $\delta(x) \geq m$ per ogni $x \in A^*$.

(b) $\delta(a) = m$ per ogni elemento invertibile a di A.

D'altra parte, se $a, b \in A^*$, $b|a$ e $\delta(a) = \delta(b)$ allora $a \sim b$ per l'esercizio 11.8. Questo implica facilmente che

(c) $\delta(x) > m$ per ogni elemento non invertibile x di A.

In altre parole, i valori di δ sono "concentrati" in m, per gli elementi invertibili, oppure sono maggiori di m, per gli elementi non invertibili. Per semplificare possiamo definire un nuova norma δ^* ponendo $\delta^*(a) = \delta(a) - m$ per ogni $a \in A^*$. Con questa norma A risulta un dominio euclideo e inoltre $\delta^*(1) = 0$.

Osserviamo infine che se A è un dominio euclideo tale che $\delta(A^*)$ è finito, allora A è un campo. Supponiamo per assurdo che esista $b \neq 0$ non invertibile, allora $b^n \neq 1$ per ogni $n \in \mathbb{N}$. Da questo segue facilmente che $\delta(b^{n+1}) > \delta(b^n)$ per ogni $n \in \mathbb{N}$. Pertanto l'insieme $\delta(A^*)$ è infinito.

Teorema 11.36. *Ogni dominio euclideo è principale.*

DIMOSTRAZIONE. Sia A un dominio euclideo con norma δ. L'ideale nullo è principale, pertanto sia I un ideale non banale. Tra gli elementi non nulli $a \in I$ scegliamo l'elemento a_0 con il minimo valore di $\delta(a_0)$. Dimostreremo che $I = (a_0)$. Si ha $(a_0) \subseteq I$. Sia $a \in I$, allora esistono $q, r \in A$, tali che $a = qa_0 + r$ e $r = 0$ oppure $r \neq 0$ e $\delta(r) < \delta(a)$. Poiché $\delta(a_0)$ è stato scelto come minimo valore e poiché $r = a - qa_0 \in I$, la seconda possibilità non può essere verificata. Resta dunque $r = 0$ e quindi $a = qa_0 \in (a_0)$. □

Il seguente teorema 11.37 si ottiene facilmente come corollario dei teoremi 11.28 e 11.36. Diamo comunque una dimostrazione diretta.

Teorema 11.37. *Ogni dominio euclideo è fattoriale.*

DIMOSTRAZIONE. Sia A un dominio euclideo relativo alla norma $\delta : A^* \to \mathbb{N}$. Non è restrittivo supporre che $\delta(1) = 0$. Per un elemento non invertibile $a \in A$ dimostriamo che a ha una fattorizzazione unica in prodotto di elementi irriducibili. Ragioniamo per induzione su $\delta(a)$. Il caso $\delta(a) = 0$ è banale perché

$$1|a \text{ e } \delta(a) = 0 = \delta(1)$$

implicano che a è invertibile per l'esercizio 11.8. Supponiamo $\delta(a) > 0$. Se a è irriducibile abbiamo finito. Altrimenti $a = bc$ con b e c non invertibili, cioè $a \not\sim b$, $a \not\sim c$. Allora $\delta(b) < \delta(a)$ e $\delta(c) < \delta(a)$ per l'esercizio 11.8. Per l'ipotesi induttiva, entrambi b e c, non essendo invertibili, sono prodotti di elementi irriducibili e pertanto anche a è prodotto di elementi irriducibili.

Per dimostrare l'unicità ricordiamo che in un dominio principale ogni elemento irriducibile è anche primo. Si conclude per il lemma 11.16. □

Si noti come nella definizione di dominio euclideo e nelle precedenti dimostrazioni ci siano diverse analogie con l'anello degli interi. Vediamo ora un altro esempio di anello euclideo.

Definizione 11.38. L'anello $\mathbb{Z}[i]$ dei *numeri di Gauss* è il sottoinsieme dei numeri complessi del tipo $a+ib$, ove $a, b \in \mathbb{Z}$ e $i^2 = -1$, che si verifica essere un sottoanello di $\mathbb{C}$.

Teorema 11.39. *L'anello $\mathbb{Z}[i]$ è un dominio euclideo con la norma δ definita da $\delta(z) = a^2 + b^2$, per $z = a + ib \in \mathbb{Z}[i]$.*

DIMOSTRAZIONE. Innanzitutto $\mathbb{Z}[i]$ è un dominio, in quanto è un sottoanello di $\mathbb{C}$. Si verifica facilmente che $\delta(z) \in \mathbb{N}$ e $\delta(zw) = \delta(z)\delta(w)$ per ogni $z, w \in \mathbb{Z}[i]$. Infatti $\delta(z) = |z|^2$ e $\delta(zw) = \delta(z)\delta(w)$ in quanto il modulo dei numeri complessi preserva la moltiplicazione. Per verificare che $\mathbb{Z}[i]$ è un dominio euclideo, osserviamo che se $w \neq 0$, allora $w^{-1} = \delta(w)^{-1}\overline{w}$, ove $\overline{w}$ è il coniugato di w. Quindi esistono $\alpha, \beta \in \mathbb{Q}$ tali che $zw^{-1} = \alpha + i\beta$. Possiamo ora trovare degli interi u, v tali che

$$|u - \alpha| \leq 1/2 \quad \text{e} \quad |v - \beta| \leq 1/2.$$

Allora

$$\begin{aligned} z = w(\alpha + i\beta) &= w\left((\alpha - u + u) + i(\beta - v + v)\right) = \\ &= w(u + iv) + w\left((\alpha - u) + i(\beta - v)\right). \end{aligned}$$

Se poniamo $q = u + iv$ e $r = w[(\alpha - u) + i(\beta - v)]$, allora $z = qw + r$, $q \in \mathbb{Z}[i]$ e $r \in \mathbb{Z}[i]$ perché differenza di elementi in $\mathbb{Z}[i]$. Resta da provare la condizione su r:

$$\delta(r) = |w|^2[(\alpha - u)^2 + (\beta - v)^2] \leq |w|^2\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}\delta(w) < \delta(w).$$

Concludiamo che $\mathbb{Z}[i]$ è un dominio euclideo. □

Utilizzando il fatto che i numeri di Gauss sono un dominio euclideo, diamo una nuova dimostrazione di una proprietà notevole dei numeri primi del tipo $p = 4k + 1$, che era già stata provata nella proposizione 3.52.

Teorema 11.40. *I numeri primi del tipo $p = 4k + 1$ si possono presentare come somma di due quadrati.*

DIMOSTRAZIONE. Sia p un numero primo del tipo $p = 4k + 1$. Per il teorema di Wilson 3.49 si ha

$$(p-1)! \equiv_p -1.$$

Osserviamo che per ogni j tra 1 e $a = \frac{p-1}{2}$, si ha $j(p-j) \equiv_p -j^2$. Pertanto, se consideriamo $b = a!$ si ottiene:

$$-1 \equiv_p (p-1)! = 1 \cdot 2 \cdot \dots \cdot j \cdot \dots \cdot a \cdot (p-a) \cdot \dots \cdot (p-j) \cdot \dots \cdot (p-1) \equiv_p$$

$$\equiv_p (a!) \cdot (-1)^{\frac{p-1}{2}} \cdot (a!) \equiv_p b^2.$$

Consideriamo ora il dominio euclideo $\mathbb{Z}[i]$. Dal fatto che p divide b^2+1, segue che $p|(b+i)(b-i)$ in $\mathbb{Z}[i]$, mentre ovviamente p non divide $b+i$ e p non divide $b-i$. Quindi p non è primo. Poiché $\mathbb{Z}[i]$ è un dominio a ideali principali p non è nemmeno irriducibile. Esistono quindi $\alpha, \beta \in \mathbb{Z}[i]$, entrambi non invertibili, cioè $|\alpha| > 1$ e $|\beta| > 1$, tali che $p = \alpha\beta$. Da $p = \alpha\beta$ ricaviamo $p^2 = |\alpha|^2|\beta|^2$. Se $\alpha = x + iy$ e $\beta = u + iv$ con $x, y, u, v \in \mathbb{Z}$, si ha $p^2 = (x^2+y^2)(u^2+v^2)$. Da $|\alpha| > 1$ e $|\beta| > 1$ ricaviamo $x^2+y^2 > 1$ e $u^2+v^2 > 1$. Pertanto $p = x^2+y^2$, come si voleva dimostrare. □

Vediamo infine un esempio di domini principali che sono sempre euclidei.

Esempio 11.41. Sia A un dominio principale e $P(A)$ l'insieme dei rappresentanti degli elementi irriducibili di A, a meno di associati. Supponiamo $P(A) = \{p\}$, si veda per esempio il dominio considerato nell'esercizio 9.49. Ogni elemento non nullo di A si può scrivere come $a = up^n$, dove $u \in U(A)$ e $n \in \mathbb{N}$. Definiamo $\delta : A^* \to \mathbb{N}$ con $\delta(a) = n$. Poiché $a \sim p^n$, è chiaro che $b = vp^m$ con $v \in U(A)$ e $m \in \mathbb{N}$ divide a se e solo se $m \leq n$. Quindi la relazione $|$ è un preordine totale, cioè per $a, b \in A^*$si ha $a|b$ oppure $b|a$. Inoltre, per $a, b \in A^*$ valgono le seguenti proprietà:

(1) $\delta(ab) = \delta(a) + \delta(b)$;
(2) $\delta(a+b) \geq \min\{\delta(a), \delta(b)\}$, per $b \neq -a$.

Pertanto A risulta un dominio euclideo. I domini euclidei con le proprietà (1) e (2) si chiamano *domini di valutazione discreta.*

11.5 Divisibilità nell'anello dei polinomi, radici di un polinomio

Siano A un anello commutativo unitario ed $f(x)$ un polinomio a coefficienti in A, con

$$f = f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n \in A[x].$$

Sia $a \in B$, ove B è un anello che contiene A. Denotiamo con $f(a)$ l'elemento di B così definito:

$$f(a) = \sum_{i=0}^{n} a_i a^i = a_0 + a_1 a + \cdots + a_n a^n \in B.$$

Definizione 11.42. Siano B ed A anelli, con $B \supseteq A$ e $a \in B$. Allora a si dice *radice di* $f(x)$ o anche *zero di* $f(x)$ se $f(a) = 0$.

Diamo ora un utile criterio di divisibilità per polinomi di primo grado.

Teorema 11.43. (Teorema di Ruffini) *Siano A un dominio, $a \in A$, $f(x) \in A[x]$. Il polinomio $x - a$ divide $f(x)$ se e solo se $f(a) = 0$.*

DIMOSTRAZIONE. Per il lemma 11.9 esistono polinomi $q(x), r(x) \in A[x]$ tali che

$$f(x) = (x - a)q(x) + r(x) \tag{3}$$

e $\deg r < 1 = \deg (x - a)$ nel caso in cui $r(x) \neq 0$. In altre parole, in entrambi i casi, $r(x)$ è un elemento di A, essendo $r(x) = 0$ oppure un polinomio di grado 0. Per determinare il valore preciso di questo elemento di A calcoliamo il valore di $f(a)$ usando l'uguaglianza (3). Troviamo $f(a) = r(a)$. Poiché $x - a$ divide $f(x)$ se e solo se $r(x) = 0$, concludiamo che $x - a$ divide $f(x)$ se e solo se $f(a) = 0$. □

Nel seguito A sarà sempre un dominio o un campo. I polinomi di grado 1 in $A[x]$ sono utili al fine di descrivere la divisibilità nel dominio A. Infatti per due elementi $a, b \in A^*$ consideriamo il polinomio $f(x) = ax - b$. È facile vedere che $f(x)$ ha radici in A se e solo se a divide b. Per quanto riguarda la divisibilità in $A[x]$, chiaramente ogni polinomio di grado 1 è irriducibile. Vedremo nel seguito che questi possono essere tutti e soli i polinomi irriducibili in $A[x]$, quando A è un campo con particolari proprietà. Dal teorema di Ruffini segue immediatamente che un polinomio irriducibile di grado > 1 non può avere radici, tuttavia un polinomio $f(x)$ senza radici potrebbe anche non essere irriducibile. Se $\deg f \leq 3$, allora $f(x)$ è irriducibile se e solo se $f(x)$ non ha radici in A.

Determiniamo un limite superiore per il numero delle radici distinte di un polinomio.

Teorema 11.44. *Sia A un dominio e sia $f(x)$ un polinomio su A di grado $n > 0$. Allora $f(x)$ può avere al più n radici distinte.*

DIMOSTRAZIONE. Dimostriamo il teorema per induzione sul grado n. Se $n = 1$ e a è una radice di $f(x)$, per il teorema di Ruffini $x - a$ divide $f(x)$ e pertanto $f(x) = c(x - a)$, con $c \in A^*$, da cui segue che a è l'unica radice di $f(x)$. Supponiamo $n > 1$. Siano $a_1, \ldots, a_m$ le radici distinte di f. Per il teorema di Ruffini $x - a_1$ divide $f(x)$ e quindi $f(x) = (x - a_1)g(x)$, dove $g(x) \in A[x]$. Poiché $a_i \neq a_1$, abbiamo $a_i - a_1 \neq 0$ per ogni $i = 2, \ldots m$. Allora ricaviamo

$$0 = f(a_i) = (a_i - a_1)g(a_i).$$

Poiché A è un dominio, possiamo concludere che $g(a_i) = 0$ per ogni $i = 2, \ldots, m$.
Ora per ipotesi induttiva, poiché il grado di $g(x)$ è $n - 1$, segue che $g(x)$ ha la più $n-1$ radici distinte. Pertanto, poiché ogni radice di $f(x)$ diversa da a_1 è anche radice di $g(x)$, segue che $f(x)$ ha al più n radici. □

La commutatività del dominio A è essenziale nel teorema 11.44. Infatti, come si deduce facilmente dall'esercizio 9.10 il polinomio $x^2 + 1$ di grado due ha infinite radici nel corpo dei quaternioni $\mathbb{H}$ che riempiono l'intera sfera unitaria in $\mathbb{R}^3$, si veda anche l'esercizio 9.11.

Vedremo nel seguente corollario del teorema 11.44 che se i valori di due polinomi di grado al più n coincidono per più di n elementi distinti del dominio, allora i polinomi coincidono. Questa proprietà importante si chiama *principio di identità dei polinomi.*

Corollario 11.45. *Sia A un dominio e siano $f(x), g(x)$ due polinomi non costanti a coefficienti in A di grado al più $n > 0$. Se $a_0, a_1, \dots, a_n$ sono elementi distinti di A, con $f(a_i) = g(a_i)$ per ogni $i = 0, 1, ..., n$, allora $f(x) = g(x)$.*

DIMOSTRAZIONE. Poniamo $h(x) = f(x) - g(x)$. Allora $h(x)$ è un polinomio di grado al più n. Se il grado di h è 0, allora $h(x)$ è costante, e questa costante è proprio 0 perché $h(a_i) = 0$ per $i = 0, 1, \dots, n$. Questo dimostra che $f(x) = g(x)$. Supponiamo ora, per assurdo, che il grado di h sia positivo. D'altra parte $h(x)$ ha $n + 1$ radici $a_0, a_1, \dots, a_n$, che contraddice il teorema 11.44. □

Un'altra utile applicazione del teorema 11.44 si ottiene per i campi finiti.

Corollario 11.46. *Sia F un campo finito. Allora il gruppo moltiplicativo $(F^*, \cdot)$ è ciclico.*

DIMOSTRAZIONE. Denotiamo con n l'ordine del gruppo abeliano $G = (F^*, \cdot)$. Ragionando per assurdo supponiamo che G non sia ciclico. Allora esiste un divisore proprio d di n tale che ogni elemento x di G soddisfa $x^d = 1$ per l'esercizio 7.30. Pertanto il polinomio $f(x) = x^d - 1$ ha $n > d$ radici in F, assurdo per il teorema 11.44. □

Un'altra applicazione del teorema di Ruffini permette di dare una seconda dimostrazione del teorema di Wilson.

Corollario 11.47. *Sia p un numero primo. Allora*

(a) il polinomio $x^p - x \in \mathbb{F}_p[x]$ si scompone in

$$x^p - x = x(x-1)(x-2)\dots(x-p+1).$$

(b) p divide $(p-1)! + 1$.

DIMOSTRAZIONE. (a) La fattorizzazione $x^p - x = x(x-1)(x-2)\dots(x-p+1)$ si ricava ragionando come nella dimostrazione del teorema 11.44.

(b) Dalla fattorizzazione del punto (a) e dal corollario 11.45 concludiamo che i coefficienti di x in entrambi polinomi coincidono. Pertanto si ha la congruenza $-1 \equiv_p (p-1)!$. □

Quando A è un campo, l'anello $A[x]$ ha ottime proprietà per quanto riguarda la divisibilità. Infatti un esempio molto importante di dominio euclideo è l'anello dei polinomi definiti su un campo K. Sia dunque K un campo. La funzione grado

definita sugli elementi non zero di $K[x]$, fornisce la funzione δ necessaria affinchè $K[x]$ sia un anello euclideo. Siamo ora nelle condizioni di poter provare che l'anello $K[x]$ risulta essere un dominio euclideo, nel caso in cui K è un campo.

Teorema 11.48. *Sia K un campo. Allora $K[x]$ è un dominio euclideo.*

DIMOSTRAZIONE. Per il corollario 11.8 $K[x]$ è un dominio di integrità e per il lemma 11.9 $K[x]$ è un dominio euclideo. □

Pertanto tutti i risultati ottenuti nel caso generale di un dominio euclideo si applicano all'anello dei polinomi a coefficienti in un campo.

11.6 Fattorizzazione negli anelli di polinomi

Abbiamo visto che gli anelli di polinomi sopra un campo sono domini euclidei. In questo paragrafo consideriamo la fattorizzazione negli anelli di polinomi sopra un dominio che non sia necessariamente un campo. Studieremo infatti anelli di polinomi $A[x]$ fattoriali. È facile vedere che se $A[x]$ è fattoriale, lo è anche A. Pertanto nel seguito A denoterà sempre un dominio fattoriale.

Si prova facilmente che $U(A[x]) = U(A)$. Da questo segue che, per $a, b \in A^*$, si ha $a \sim b$ se e solo se a e b sono associati, considerati come due polinomi di grado 0 in $A[x]$. Per questo motivo la notazione $\sim$ sarà adottata anche per il dominio $A[x]$.

Definizione 11.49. Il massimo comun divisore di $a_0, a_1, \ldots, a_n$ si chiama *contenuto* di $f(x)$ e si denota con $\text{cont}\,(f)$.

Si noti che $\text{cont}\,(f)$, essendo un massimo comun divisore, è determinato a meno di un fattore invertibile in A. Ogni polinomio monico ha contenuto 1. Più in generale un polinomio $f(x) \neq 0$ si dice *primitivo* se $\text{cont}\,(f) = 1$.

Se scriviamo $f(x) = \text{cont}\,(f) f_1(x)$, il polinomio $f_1(x) \in A[x]$ determinato dalla divisione per $\text{cont}\,(f)$ dei coefficienti di $f(x)$ è primitivo. Si noti che se A è un campo, allora tutti i polinomi non nulli sono primitivi. Supponiamo ora che A non sia un campo. Allora un polinomio $f(x) \in A[x]$ è non primitivo se esiste un primo $p \in A$ tale che p divide $f(x)$. Dire che p è primo equivale a dire che l'ideale (p) di A è primo, cioè che $A/(p)$ è un dominio. Così tale è anche $(A/(p))[x]$ ed ha quindi senso considerare la naturale *p-proiezione* di $A[x]$ in $(A/(p))[x]$

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in A[x] \longmapsto \overline{f}(x) = \overline{a_0} + \overline{a_1} x + \ldots + \overline{a_n} x^n, \quad (5)$$

dove con un simbolo del tipo $\overline{a}$ si intende la classe di equivalenza di a modulo (p), cioè $a + (p)$. La p-proiezione (5) risulta essere un omomorfismo suriettivo di anelli il cui nucleo è costituito dai polinomi che ammettono p come divisore. Allora un polinomio è primitivo se e solo se non si annulla in alcuna p-proiezione.

Dimostriamo come la conoscenza dei polinomi irriducibili sul quoziente $A/(p)$ permette talvolta di trovare polinomi irriducibili su A.

Lemma 11.50. *Sia A un dominio fattoriale, $p \in A$ un elemento primo e*

$$f(x) = a_0 + a_1x + \ldots + a_nx^n$$

un polinomio primitivo su A con $(p, a_n) = 1$. Sia

$$\overline{f}(x) = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_n}x^n$$

la p-proiezione di f in $(A/(p))[x]$ come definita in (5). Se $\overline{f}(x)$ è irriducibile in $(A/(p))[x]$, allora anche $f(x)$ è irriducibile in $A[x]$.

DIMOSTRAZIONE. Sia $f(x) = g(x)h(x)$ una fattorizzazione di $f(x)$ in $A[x]$ con

$$g(x) = b_0 + b_1x + \ldots + b_kx^k \quad \text{e} \quad h(x) = c_0 + c_1x + \ldots + c_mx^m,$$

$k = \deg g > 0$ e $m = \deg h > 0$. Si ha $k + m = n$ e $b_kc_m = a_n \neq 0$, da cui segue che p non divide b_k e p non divide c_m, in quanto A è un dominio e per ipotesi p non divide a_n. "Proiettando" la fattorizzazione $f(x) = g(x)h(x)$ tramite l'omomorfismo canonico $A[x] \to B[x]$ otteniamo una fattorizzazione $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $B[x]$ con

$$\overline{g}(x) = \overline{b}_0 + \overline{b}_1x + \ldots + \overline{b}_kx^k \quad \text{e} \quad \overline{h}(x) = \overline{c}_0 + \overline{c}_1x + \ldots + \overline{c}_mx^m,$$

con $\overline{b_k} \neq 0 \neq \overline{c_m}$. Poiché $k = \deg \overline{g} > 0$ e $m = \deg \overline{h} > 0$, questo contraddice l'irriducibilità di $\overline{f}$. □

Non è ora difficile dimostrare il "lemma di Gauss", cui premettiamo un facile lemma sul confronto di polinomi primitivi.

Lemma 11.51. *Se $f(x), g(x) \in A[x]$ sono polinomi primitivi, $a, b \in A^*$ e $af(x) = bg(x)$ o, più in generale, $af(x) \sim bg(x)$, allora $a \sim b$ e $f(x) \sim g(x)$.*

DIMOSTRAZIONE. Poiché $f(x)$ è primitivo, b divide a. Poiché anche $g(x)$ è primitivo, risulta che anche a divide b. Quindi $a \sim b$ e $f(x) \sim g(x)$. □

Lemma 11.52. (Lemma di Gauss) *Sia A un dominio fattoriale e $A[x]$ il suo anello dei polinomi. Allora il prodotto di polinomi primitivi di $A[x]$ è un polinomio primitivo.*

DIMOSTRAZIONE. Supponiamo che $f(x), g(x) \in A[x]$ siano polinomi primitivi e che, per assurdo, il loro prodotto $h(x) = f(x)g(x)$ non sia primitivo. Allora una sua p-proiezione $\overline{h}(x) = \overline{f}(x)\overline{g}(x) = 0 \in A/(p)[x]$ è nulla. Poiché l'anello quoziente $A/(p)$ è un dominio, in quanto (p) è un ideale primo di A, anche l'anello $A/(p)[x]$ è un dominio. Quindi uno dei due polinomi $\overline{f}(x)$, $\overline{g}(x)$ è nullo, cioè $f(x)$ o $g(x)$ non è primitivo, assurdo. □

Siano A un dominio fattoriale e K il suo campo dei quozienti. Dato un polinomio $f(x) = r_0 + r_1x + \ldots + r_nx^n \in K[x]$ esistono $a_i, b_i \in A$ tali che $r_i = \frac{a_i}{b_i}$ per ogni $i = 0, ..., n$, come dimostrato nel paragrafo 10.3. Ricordiamo che $\frac{a_i}{b_i} = a_ib_i^{-1}$. Sia

$b = b_0 \ldots b_n$, allora $g(x) = bf(x) \in A[x]$ e $f(x) = \frac{1}{b} \cdot g(x)$. Se poniamo $a = \mathrm{cont}\,(g)$, possiamo scrivere

$$f(x) = \frac{a}{b} \cdot \tilde{f}(x), \tag{6}$$

dove $\tilde{f}(x) \in A[x]$ è un polinomio primitivo con $\deg \tilde{f} = \deg f$.

Lemma 11.53. *Sia A un dominio fattoriale e sia K il suo campo dei quozienti. Se $f(x) \in A[x]$ è primitivo e divide il polinomio $g(x) \in A[x]$ in $K[x]$, allora $f(x)$ lo divide anche in $A[x]$.*

DIMOSTRAZIONE. Sia $g(x) = f(x) \cdot h(x)$ con $h(x) \in K[x]$. Allora esiste $a \in A$ con $h_1(x) = a \cdot h(x) \in A[x]$. Quindi $a \cdot g(x) = f(x) \cdot h_1(x)$. Dimostriamo che $h(x) \in A[x]$. Per l'esercizio 11.19, $a \cdot \mathrm{cont}\,(g(x)) \sim 1 \cdot \mathrm{cont}\,(h_1(x))$. Di conseguenza a divide $\mathrm{cont}\,(h_1(x))$. Pertanto il polinomio $a^{-1} \cdot h_1(x) = h(x)$ appartiene ad $A[x]$ e $f(x)$ divide $g(x)$ in $A[x]$. □

11.7 Polinomi irriducibili su un dominio fattoriale

Il seguente teorema descrive i polinomi irriducibili sopra un dominio fattoriale tramite i polinomi irriducibili sopra il suo campo dei quozienti.

Teorema 11.54. *Siano A un dominio fattoriale e K il suo campo dei quozienti. Un polinomio $f(x) \in A[x]$ di grado > 0 è irriducibile in $A[x]$ se e solo se $f(x)$ è primitivo e irriducibile in $K[x]$.*

DIMOSTRAZIONE. Sia $f(x) \in A[x]$ irriducibile in $A[x]$. Allora $f(x)$ è primitivo. Supponiamo che $f(x) = g(x) \cdot h(x)$ sia una fattorizzazione in $K[x]$. Siano

$$g(x) = \frac{a}{b} \cdot \tilde{g}(x) \quad \text{e} \quad h(x) = \frac{a'}{b'} \cdot \tilde{h}(x)$$

le presentazioni come in (6). Allora si ha

$$bb' \cdot f(x) = aa' \cdot \tilde{g}(x) \cdot \tilde{h}(x).$$

Per il lemma 11.52 il polinomio $\tilde{g}(x) \cdot \tilde{h}(x)$ è primitivo, quindi $f(x) \sim \tilde{g}(x) \cdot \tilde{h}(x)$ per il lemma 11.51. Questo implica una fattorizzazione di $f(x)$ in $A[x]$. Per ipotesi $f(x)$ è irriducibile in $A[x]$, quindi uno dei due polinomi $\tilde{g}(x)$, $\tilde{h}(x)$ è di grado zero. Di conseguenza lo stesso vale anche per $g(x)$ e $h(x)$. Questo dimostra che $f(x)$ è irriducibile in $K[x]$. Supponiamo adesso che $f(x) \in A[x]$ sia irriducibile in $K[x]$. Allora una fattorizzazione $f(x) = g(x) \cdot h(x)$ in $A[x]$ può avvenire solo se $\deg g(x) = 0$, cioè $g(x) = a \in A$. Se inoltre sappiamo che $f(x)$ è primitivo, possiamo concludere che $a \in A$ è invertibile in A. Questo dimostra che $f(x)$ è irriducibile in $A[x]$. □

Consideriamo ora il caso di grado 0 che non è stato trattato dal teorema 11.54. I polinomi di grado 0 in $A[x]$ sono gli elementi $a \in A$. Poiché una fattorizzazione

$a = g(x) \cdot h(x)$ può avvenire soltanto con polinomi di grado 0, cioè elementi di A, concludiamo che a è irriducibile in $A[x]$ se e solo se a è irriducibile in A. In questo modo abbiamo descritto *tutti* i polinomi irriducibili di $A[x]$.

Abbiamo già visto nel teorema 11.48 che l'anello dei polinomi sopra un campo è un anello euclideo e pertanto un dominio principale per il teorema 11.36. In generale, se A è un dominio, non è detto che $A[x]$ sia un dominio euclideo, come mostra il seguente esempio.

Esempio 11.55. Sia F un campo. Allora l'anello dei polinomi $A = F[x]$ su F è un dominio di integrità. Possiamo definire anche il suo anello dei polinomi

$$A[y] = F[x][y] = F[x, y].$$

Se $A[y]$ fosse un dominio euclideo, in particolare sarebbe un dominio a ideali principali, mentre l'ideale $I = (x, y)$ di $A[y]$ non è principale.

Ha senso pertanto chiedersi quali proprietà dell'anello A vengono conservate nell'anello $A[x]$.

Teorema 11.56. *L'anello di polinomi sopra un dominio fattoriale è un dominio fattoriale.*

DIMOSTRAZIONE. Sia A un dominio fattoriale e K il suo campo dei quozienti. Sia $f(x) \in A[x]$. Dimostriamo che $f(x)$ si fattorizza, in modo unico, in prodotto di polinomi irriducibili in $A[x]$. Procediamo per induzione sul grado $d = \deg f$. Se $d = 0$, allora l'esistenza della fattorizzazione segue dall'esistenza della fattorizzazione in A. Analogamente, per l'unicità: tutti i polinomi in una fattorizzazione di $f(x)$ in questo caso sono elementi di A e allora l'unicità segue dall'unicità della fattorizzazione in A. Sia $d > 0$. Scriviamo $f(x) = \text{cont}(f) f_1(x)$ e fattorizziamo $\text{cont}(f) = p_1 \dots p_n$ in prodotto di elementi irriducibili di A e quindi irriducibili in $A[x]$. Se anche $f_1(x)$ è irriducibile in $A[x]$, abbiamo finito. Altrimenti esistono $g(x), h(x) \in A[x]$ con

$$f_1(x) = g(x) \cdot h(x) \quad \text{e} \quad f(x) \not\sim g(x), \quad f(x) \not\sim h(x).$$

Poiché $f_1(x)$ è primitivo, questo implica $\deg g(x) < d$ e $\deg h(x) < d$. Applichiamo l'ipotesi induttiva a $g(x)$ ed $h(x)$ per trovare così una fattorizzazione anche di $f(x)$.

Sia $f(x) = g_1(x) \dots g_n(x)$ una fattorizzazione in prodotto di polinomi irriducibili in $A[x]$. Dimostriamo che essa è unica. Per l'ipotesi $d > 0$ almeno uno dei fattori, diciamo $g_1(x)$, ha grado > 0. Supponiamo ora che $f(x) = h_1(x) \dots h_m(x)$ sia un'altra fattorizzazione in prodotto di polinomi irriducibili di f in $A[x]$. Poiché $g_1(x)$ è un polinomio irriducibile di $K[x]$ per il teorema 11.54 e in $K[x]$ gli elementi irriducibili sono anche primi, possiamo concludere che $g_1(x)$ divide, in $K[x]$, uno dei fattori nella seconda fattorizzazione, diciamo $h_1(x)$. Per il lemma 11.53 concludiamo che $g_1(x)$ divide $h_1(x)$ anche in $A[x]$. Sia $q(x)$ il risultato di questa divisione. Poiché $h_1(x)$ è irriducibile per ipotesi, sappiamo pure che $q(x) \in U(A[x])$. Allora avremo

$$g_2(x) \cdot \dots \cdot g_n(x) = q(x) \cdot h_2(x) \cdot \dots \cdot h_m(x) \sim h_2(x) \cdot \dots \cdot h_m(x).$$

Poiché il grado del polinomio $g_2(x) \cdot \dots \cdot g_n(x)$ è minore di d, concludiamo che $m = n$ e, a meno di permutazione, $g_i(x) \sim h_i(x)$ per $1 < i \leq n$. □

Essendo $\mathbb{Z}$ un dominio euclideo, e quindi fattoriale per il teorema 11.28, i risultati del paragrafo precedente si applicano anche al caso $A = \mathbb{Z}$ e $K = \mathbb{Q}$.

Teorema 11.57. *L'anello di polinomi $\mathbb{Z}[x]$ è fattoriale. Un polinomio $f(x) \in \mathbb{Z}[x]$ è irriducibile in $\mathbb{Z}[x]$ se e solo se $f(x)$ è primitivo ed è irriducibile in $\mathbb{Q}[x]$.*

L'anello $\mathbb{Z}[x]$ non è euclideo in virtù del fatto di avere ideali non principali, per esempio l'ideale $(2, x)$. Ci si potrebbe domandare allora come si giustifica il passaggio dall'anello $\mathbb{Q}[x]$, dominio euclideo, all'anello $\mathbb{Z}[x]$. Il vantaggio di lavorare in $\mathbb{Z}[x]$ è la possibilità di proiettare le fattorizzazioni in $\mathbb{Z}[x]$ in fattorizzazioni in $\mathbb{F}_p[x]$, tramite l'omomorfismo canonico $\mathbb{Z}[x] \to \mathbb{F}_p[x]$, ottenuto facendo il quoziente dell'anello $\mathbb{Z}[x]$ tramite l'ideale principale (p), generato dal primo p. Allora utilizzando il lemma 11.50, la conoscenza dei polinomi irriducibili sul campo finito $\mathbb{F}_p$ permette talvolta di trovare polinomi irriducibili su $\mathbb{Z}$ e quindi su $\mathbb{Q}$.

Mostriamo ora un'utile condizione sufficiente per l'irriducibilità di alcuni polinomi, nota come *criterio di Eisenstein.* Si tratta di polinomi il cui grado viene mantenuto in una p-proiezione.

Lemma 11.58. (Criterio di Eisenstein) *Sia A un dominio principale, sia*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

un polinomio primitivo su A e sia $p \in A$ un elemento primo tale che:

(a) p divide $a_0, a_1, \ldots, a_{n-1}$;
(b) p non divide a_n;
(c) p^2 non divide a_0.

Allora il polinomio $f(x)$ è irriducibile in $A[x]$.

DIMOSTRAZIONE. L'ideale (p), essendo primo e non nullo, è massimale. Quindi il quoziente $B = A/(p)$ è un campo. Allora il quoziente $A[x]/pA[x]$, essendo isomorfo a $B[x]$, è un dominio euclideo. Sia $f(x) = g(x)h(x)$ una fattorizzazione di $f(x)$ in $A[x]$ con

$$g(x) = b_0 + b_1 x + \ldots + b_k x^k \quad \text{e} \quad h(x) = c_0 + c_1 x + \ldots + c_m x^m,$$

$k = \deg g > 0$ e $m = \deg h > 0$. Si ha $k + m = n$ e $b_k c_m = a_n \neq 0$, quindi (b) implica che p non divide b_k e p non divide c_m. "Proiettando" la fattorizzazione $f(x) = g(x)h(x)$ tramite l'omomorfismo canonico $A[x] \to B[x]$ otteniamo una fattorizzazione $\overline{a}_n x^n = \overline{g}(x)\overline{h}(x)$ in $B[x]$ con

$$\overline{g}(x) = \overline{b}_0 + \overline{b}_1 x + \ldots + \overline{b}_k x^k \quad \text{e} \quad \overline{h}(x) = \overline{c}_0 + \overline{c}_1 x + \ldots + \overline{c}_m x^m.$$

Osserviamo che entrambi i polinomi $\overline{g}(x), \overline{h}(x)$ dividono il polinomio x^n in $B[x]$ e $\overline{b}_k \neq 0$, $\overline{c}_m \neq 0$. Poiché la fattorizzazione in irriducibili in $B[x]$ è unica e l'unico

irriducibile che divide x^n è il polinomio x, possiamo concludere che $\overline{g}(x) = \overline{b}_k x^k$ e $\overline{h}(x) = \overline{c}_m x^m$ in $B[x]$. Allora i polinomi $g(x)$ e $h(x)$ si possono scrivere in $A[x]$ nella forma

$$g(x) = b_k x^k + pg_2(x), \quad h(x) = c_m x^m + ph_2(x),$$

dove $g_2(x), h_2(x) \in A[x]$ e $\deg g_2 < k$ e $\deg h_2 < m$. In tal caso il termine noto del prodotto $g(x)h(x) = f(x)$ è divisibile per p^2 contrariamente all'ipotesi di partenza. Questo dimostra che $f(x)$ è irriducibile in $A[x]$. □

Esempio 11.59. Applicheremo il criterio di Eisenstein 11.58 per provare che per ogni primo p il polinomio

$$h(x) = 1 + x + \ldots + x^{p-1} = \frac{x^p - 1}{x - 1}$$

è irriducibile in $\mathbb{Z}[x]$. Un'applicazione immediata del criterio non è possibile e per questo cercheremo di modificare opportunamente $h(x)$. Consideriamo l'applicazione $\kappa : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$ che manda ogni polinomio $f(x) \in \mathbb{Z}[x]$ nel polinomio $f(x+1)$. Ponendo $\lambda[g(x)] = g(x-1)$ per $g(x) \in \mathbb{Z}[x]$, vediamo che κ è un automorfismo di anelli di $\mathbb{Z}[x]$ con inverso λ. Poiché ogni automorfismo preserva la proprietà di essere irriducibile, osserviamo che se $h(x)$ è riducibile, allora $g(x) = h(x+1)$ è riducibile. Quindi è sufficiente dimostrare che $g(x)$ è irriducibile. Poiché

$$g(x) = h(x+1) = \frac{(x+1)^p - 1}{x} = \frac{1}{x}\left(\sum_{k=0}^{p}\binom{p}{k}x^k - 1\right) = \sum_{k=1}^{p}\binom{p}{k}x^{k-1},$$

il polinomio $g(x)$ risulta irriducibile per il criterio di Eisenstein, pertanto $h(x)$ è irriducibile in $\mathbb{Z}[x]$.

Nel paragrafo 12.10 sono riassunti alcuni criteri utili per discutere la riducibilità dei polinomi.

11.8 Esercizi su anelli di polinomi

Esercizio 11.1 Sia A un anello commutativo unitario. Dimostrare che

$$\operatorname{char} A[x] = \operatorname{char} A.$$

Se A è un campo, allora anche $\operatorname{char} A(x) = \operatorname{char} A$.

Esercizio 11.2 Sia A un anello commutativo unitario. Dimostrare che $f(x) \in A[x]$ è nilpotente se e solo se tutti i coefficienti di f sono nilpotenti.

Esercizio 11.3 Sia A un anello commutativo unitario e sia $f(x) \in A[x]$ con coefficiente direttivo invertibile e di grado $n > 0$.

(a) Dimostrare che, dato l'ideale principale $I = (f(x))$, esiste una biezione tra l'anello quoziente $A[x]/I$ e le classi laterali $r(x) + I$, dove $r(x)$ è un polinomio di grado $< n$ oppure $r(x) = 0$.
(b) Calcolare la cardinalità degli anelli quoziente $\mathbb{Z}_2[x]/(x^3+x+1)$, $\mathbb{Z}_3[x]/(x^2-1)$, $\mathbb{Z}_5[x]/(x^6 - x^2 + x - 1)$.

Esercizio 11.4 Sia A un dominio. Dimostrare che $U(A[x]) = U(A)$. Resta vera questa uguaglianza se A non è un dominio?

Esercizio 11.5 Sia A un anello commutativo unitario e sia I un ideale di A. Sia J l'insieme di tutti polinomi che hanno tutti i coefficienti in I. Dimostrare che J è un ideale di $A[x]$ e $A[x]/J \cong (A/I)[x]$.

Esercizio 11.6 Sia A il sottoanello $\mathbb{Z}[\sqrt{-3}]$ di $\mathbb{C}$ generato da $\mathbb{Z}$ e $\sqrt{-3}$. Trovare gli elementi invertibili di A e dimostrare che A non è fattoriale.

Esercizio 11.7 Siano A un dominio e B un anello unitario isomorfo ad A quale anello unitario. Si dimostri che

(a) B è un dominio;
(b) se A è fattoriale, allora anche B è fattoriale;
(c) se A è principale, allora anche B è principale;
(d) se A è euclideo, allora anche B è euclideo.

Esercizio 11.8 Sia A un dominio euclideo e $a, b \in A^*$. Se $b|a$ e $\delta(a) = \delta(b)$ allora $a \sim b$.

Esercizio 11.9 Sia A un dominio euclideo tale che per ogni $n \in \mathbb{N}$ ci sia un numero finito di elementi $a \in A^*$ con $\delta(a) \leq n$. Dimostrare che ogni ideale non nullo di A ha indice finito.

Esercizio 11.10 Sia K un campo finito. Dimostrare che ogni ideale non nullo di $K[x]$ ha indice finito.

Esercizio 11.11 Si dimostri che i numeri interi $n > 1$ per i quali esistono $a, b \in \mathbb{Z}$ tali che $n = a^2 + b^2$ non sono irriducibili nell'anello $\mathbb{Z}[i]$ dei numeri di Gauss.

Esercizio 11.12 (a) Si dimostri che i numeri primi $p > 2$, per i quali esistono $a, b \in \mathbb{Z}$ tali che $p = a^2 + b^2$, sono precisamente quelli del tipo $p = 4k + 1$.

(b) Si dimostri che i numeri primi $p \in \mathbb{Z}$ che sono irriducibili anche nell'anello $\mathbb{Z}[i]$ dei numeri di Gauss sono precisamente quelli del tipo $p = 4k + 3$.

Esercizio 11.13 Sia $z = a + ib \in \mathbb{Z}[i]$ un intero di Gauss e $\delta(z) = a^2 + b^2$. Se $\delta(z)$ è primo, allora z è irriducibile.

Esercizio 11.14 Scomporre i seguenti interi di Gauss in prodotto di primi di Gauss $2, 5, 17, 1 + 2i, 6i - 3$.

Esercizio 11.15 Determinare i numeri primi p per i quali il polinomio $x^2 + 1$ risulta irriducibile su $\mathbb{F}_p$.

Esercizio 11.16 (Lemma di Gauss, seconda forma) Se A è un dominio fattoriale e p è primo in A, allora p è primo anche in $A[x]$.

Esercizio 11.17 Sia A un dominio a ideali principali e sia I un ideale di A non banale. Dimostrare che ogni elemento non invertibile del quoziente $B = A/I$ è divisore dello zero.

Esercizio 11.18 Sia A un dominio a ideali principali. Un ideale I di A è detto *primario* se, per ogni $a, b \in A$, con $ab \in I$ e $a \notin I$, uno fra $b, b^2, b^3, \dots$ è in I. Dimostrare che I è primario se $I = (0)$, oppure $I = (p^n)$, per qualche primo $p \in A$ e qualche $n \geq 1$.

Esercizio 11.19 Dimostrare che per $f(x), g(x) \in A[x]$ si ha

$$\operatorname{cont}(f(x) \cdot g(x)) \sim \operatorname{cont}(f(x)) \cdot \operatorname{cont}(g(x)).$$

Esercizio 11.20 Sia A un dominio principale e sia $a \in A$ un elemento che ha un divisore primo $p \in A$ tale che p^2 non divide a. Allora il polinomio $f(x) = x^n + a$ è irriducibile in $A[x]$ per ogni $n > 0$.

Esercizio 11.21 Si dimostri che i polinomi $x^5 - 6x + 3$ e $x^7 - 60$ sono irriducibili in $\mathbb{Z}[x]$.

Esercizio 11.22 Siano $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi e I l'insieme dei polinomi di $\mathbb{Z}[x]$ il cui termine di grado zero è pari. Verificare che I è ideale di $\mathbb{Z}[x]$ e che I non è principale.

Esercizio 11.23 Sia p un numero primo. Dimostrare che non esiste alcun omomorfismo di anelli unitari $\mathbb{Q}[x] \to \mathbb{F}_p[x]$.

Esercizio 11.24 Dimostrare che il polinomio $x^4 + x^3 + 1 \in \mathbb{Z}[x]$ è irriducibile.

Esercizio 11.25 Dimostrare che l'ideale $(2, x^4+x^2+1)$ in $\mathbb{Z}[x]$ non è primo, mentre l'ideale $(2, x^4 + x^3 + 1)$ è primo. Quale dei due ideali è massimale?

Esercizio 11.26 Dimostrare che un ideale massimale di $\mathbb{Z}[x]$ non può essere principale.

Esercizio 11.27* Dimostrare che ogni ideale massimale dell'anello $\mathbb{Z}[x]$ ha indice finito, mentre ogni ideale massimale dell'anello $\mathbb{Q}[x]$ ha indice infinito.

Esercizio 11.28* Descrivere gli ideali massimali dell'anello $\mathbb{Z}[x]$.

Esercizio 11.29 Nell'anello $\mathbb{Z}[x]$, siano $f(x) = x^5 - x^3 + 1$ e $g(x) = x^2 + 1$ due polinomi. Calcolare il quoziente e il resto della divisione euclidea di $f(x)$ per $g(x)$ e determinare un MCD tra f e g.

Esercizio 11.30 Nell'anello $\mathbb{Z}_7[x]$, siano

$$f(x) = 3x^4 + 2x^3 + 2x + 5 \quad \text{e} \quad g(x) = 2x^2 + 5x - 1$$

due polinomi. Calcolare il quoziente e il resto della divisione euclidea di $f(x)$ per $g(x)$ e determinare un MCD tra f e g.

Esercizio 11.31 Sia $f(x) = x^3 + x + 1 \in \mathbb{Z}_5[x]$.

(a) Provare che $f(x)$ è irriducibile in $\mathbb{Z}_5[x]$.
(b) Costruire un campo con 125 elementi.
(c) Costruire un campo con 25 elementi.

Esercizio 11.32 Siano $f(x) = (x^2 - 2)^2 \in \mathbb{Q}[x]$, $I = (f)$ e $A = \mathbb{Q}[x]/I$.

(a) A è un campo?
(b) Provare che $(x + 1) + I$ è invertibile in A e calcolarne l'inverso.
(c) Sia M l'insieme degli elementi di A non invertibili. Provare che M è ideale di A.
(d) Dire se M è un ideale massimale di A.

Esercizio 11.33 Fattorizzare $f(x) = 4(x^9 - x)$ in prodotto di irriducibili in $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_3[x]$.

Esercizio 11.34 Sia p un primo. Fattorizzare in prodotto di irriducibili in $\mathbb{Z}[x]$ il polinomio $f(x) = x^p - 1$.

Esercizio 11.35 Siano $K = \mathbb{Z}_7, f(x) = x^4 + 3 \in K[x]$, $I = (f)$, $A = K[x]/I$.

(a) Provare che $x^2 + 1 + I$ è invertibile.
(b) Provare che $x^2 - 4x + 3 + I$ è divisore dello zero.
(c) Elencare gli ideali di A che contengono $x^2 - 4x + 3 + I$.

Esercizio 11.36 Dire se i polinomi $f(x) = x^4 + 830x^3 + 1002x^2 + 213x + 71$ e $g(x) = x^4 + x^3 + 2x^2 + x + 4$ sono riducibili in $\mathbb{Q}[x]$.

Esercizio 11.37 Sia $K = \mathbb{Z}_3$, $f(x) = x^4 + x^3 + x^2 - 1$. Studiare l'anello quoziente $A = K[x]/(f)$:

(a) provare che A non è un dominio;
(b) trovare gli elementi nilpotenti di A;
(c) provare che $x^2 + 1$ è invertibile;
(d) elencare tutti gli ideali di A.

Esercizio 11.38 Si considerino in $\mathbb{Z}[x]$ i polinomi

$$f(x) = x^3 + x + 1 \quad \text{e} \quad g(x) = x^4 + x^2 + 1$$

e gli ideali $I = (2, f(x))$ e $J = (2, g(x))$.

(a) Determinare quale degli ideali I e J è primo.
(b) Determinare quale degli ideali I e J è massimale.
(c) Decomporre $x^4 + x^2 + 1$ nel prodotto di fattori irriducibili in $\mathbb{Z}_7[x]$.

Esercizio 11.39 * Si provi che il polinomio $f(x) = x^2 - y^3 \in \mathbb{Q}[x, y]$ è irriducibile.

Esercizio 11.40 * Si dimostri che il polinomio $f(x, y) = x^2 + y^2 - 1$ è irriducibile in $\mathbb{Q}[x, y]$.

Esercizio 11.41 Sia A l'anello $\mathbb{R}[x,y]$. Dimostrare che l'ideale $I = (x^2 + x + 1, y^2 + y + 1)$ di A non è massimale e trovare due ideali massimali M_1 e M_2 con $I = M_1 \cap M_2$.

Esercizio 11.42 Sia $\alpha \in \mathbb{C}$ radice di un polinomio

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Dimostrare che esiste un intero $m \geq 1$ tale che $m\alpha$ è radice di un polinomio monico

$$x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 \in \mathbb{Z}[x].$$

Esercizio 11.43 Sia A un dominio a ideali principali e sia I un ideale proprio non banale di A. Provare che:

(a) $I^2 \neq I$;
(b) A/I è isomorfo ad un prodotto finito di anelli locali.

Esercizio 11.44 Sia R un anello commutativo unitario e sia G un gruppo ciclico di ordine n. Dimostrare che l'anello gruppale $R[G]$ definito nell'esercizio 9.20 è isomorfo al quoziente $R[x]/(x^n - 1)$.

Esercizio 11.45 * Sia R un anello commutativo unitario e sia G un gruppo abeliano finito. Dimostrare che l'anello gruppale $R[G]$ definito nell'esercizio 9.20 è isomorfo al quoziente

$$R[x_1, x_2, \ldots, x_n]/(x_1^{k_1} - 1, x_2^{k_2} - 1, \ldots, x_n^{k_n} - 1),$$

per un opportuno n e un'opportuna n-upla $(k_1, k_2, \ldots, k_n)$ di numeri naturali.

Esercizio 11.46 * Sia p un numero primo dispari. Provare che il gruppo $\mathrm{Aut}(\mathbb{Z}_p)$ è ciclico.

Esercizio 11.47 * Sia p un numero primo dispari. Provare che il gruppo $\mathrm{Aut}(\mathbb{Z}_{p^k})$ è ciclico per ogni intero $k > 0$.

12
Estensioni di campi

Questo capitolo è dedicato ai campi e alle estensioni dei campi in relazione al problema generale della soluzione delle equazioni polinomiali. Nel primo paragrafo introduciamo le estensioni dei campi e proviamo il teorema dei gradi per le estensioni finite. Nel secondo paragrafo dimostriamo il teorema di Kronecker che garantisce che ogni polinomio a coefficienti in un campo ammette una radice in una estensione finita del campo. Nel terzo paragrafo caratterizziamo gli elementi algebrici e le estensioni algebriche finite di un campo. Nel quarto paragrafo dimostriamo l'esistenza e l'unicità del campo di spezzamento di un polinomio su un campo K, cioè un'estensione finita di K in cui il polinomio si fattorizza in fattori lineari.

Nel sesto paragrafo viene introdotta la nozione di campo algebricamente chiuso e viene dimostrato il teorema fondamentale dell'algebra dovuto a Gauss. Il settimo paragrafo è dedicato ai polinomi ciclotomici su $\mathbb{Q}$, mentre l'ottavo ai polinomi sui campi finiti. Nel nono paragrafo si studiano gli automorfismi dei campi finiti. Infine il paragrafo 10 riassume alcuni criteri utili per discutere la riducibilità di polinomi.

12.1 Estensioni finite

È facile convincersi che fra campi di caratteristica diversa non esiste alcun *omomorfismo*, cioè applicazione che rispetta le operazioni e le unità. Campi di caratteristica diversa vivono dunque in "universi paralleli". Inoltre è facile provare che la caratteristica di un campo è 0 oppure un numero primo, così come quella di ogni dominio di integrità unitario. In genere non esporremo proprietà che dipendono dalla caratteristica, se non dal fatto che essa sia nulla o meno.

Non tutti i sottoanelli di un campo K formano un campo rispetto alle operazioni di K che lo rendono un anello unitario. Pertanto saranno chiamati *sottocampi* i sottoanelli che risultano campi in questo senso. Si vede facilmente che l'intersezione di famiglie arbitrarie di sottocampi è ancora un sottocampo. In particolare l'intersezione K_0 di tutti i sottocampi di K è il più piccolo sottocampo di K che chiameremo *sottocampo fondamentale*. Se la caratteristica di K è p il sottoanello fondamentale di K è isomorfo a $\mathbb{F}_p$ ed è di conseguenza anche un sottocampo. Nel caso char $K = 0$,

il sottoanello fondamentale di K è isomorfo a $\mathbb{Z}$ e quindi non è un campo. Pertanto il sottocampo fondamentale K_0 in questo caso è isomorfo a $\mathbb{Q}$.

Denotiamo con $K \leq E$ o $E \geq K$ o ancora E/K il fatto che K è un sottocampo del campo E e diremo anche che E è un'*estensione* di K. Le lettere E, F, L indicheranno sempre, a meno di esplicito avviso, *campi* che contengono il campo K. In questo paragrafo ci occuperemo di *estensioni di campi* e cioè delle proprietà reciproche fra i campi K ed E e, fissato K, della possibilità che esista una sua estensione E con desiderate proprietà. Come esempi di simili enunciati, da un lato vediamo subito che ogni campo E può essere visto come estensione del suo sottocampo fondamentale K e dall'altro che se $K \leq E$ è un'estensione, allora K ed E hanno la stessa caratteristica.

Se F è un'estensione del campo K, cioè $(K, +, \cdot)$ è un sottocampo di $(F, +, \cdot)$, possiamo dotare F della struttura di spazio vettoriale su K, come descritto nel lemma 4.28. A questo punto possiamo definire il grado di un'estensione.

Definizione 12.1. Sia F una estensione del campo K. Allora il *grado* di F su K è la dimensione $\dim_K F$ di F come spazio vettoriale su K e si denota con $[F : K]$.

Siano K un campo ed E un campo estensione di K, cioè $K \leq E$.

Definizione 12.2. Si dice che E/K è *un'estensione finita* se la dimensione di E come K-spazio vettoriale è finita.

Ad esempio l'estensione di campo $\mathbb{C}/\mathbb{R}$ è un'estensione finita e $[\mathbb{C} : \mathbb{R}] = 2$. Un'estensione di campo E/K può essere anche infinita: in questo caso la cardinalità di una base di E come K-spazio vettoriale è infinita. Un esempio di questo tipo è l'estensione $\mathbb{R}/\mathbb{Q}$.

Lemma 12.3. *Sia E un'estensione finita del campo K. Allora ogni campo intermedio F, cioè $K \subseteq F \subseteq E$, è un estensione finita di K.*

Teorema 12.4. (Teorema dei gradi) *Siano E un'estensione finita di K e F un'estensione finita di E. Allora F è un'estensione finita di K e*

$$[F : K] = [E : K][F : E].$$

DIMOSTRAZIONE. Sia $n = [E : K] = \dim_K E$. Allora esiste una base $\alpha_1, \dots, \alpha_n$ di E su K, cioè ogni elemento $x \in E$ ammette un'unica presentazione come combinazione lineare

$$x = \sum_{i=1}^{n} k_i \alpha_i, \quad k_i \in K. \tag{1}$$

Sia $m = [F : E] = \dim_E F$. Allora esiste una base $\beta_1, \dots, \beta_m$ di F su E, cioè ogni elemento $y \in F$ ammette un'unica presentazione come combinazione lineare

$$y = \sum_{j=1}^{m} e_j \beta_j, \quad e_j \in E. \tag{2}$$

Dimostriamo che i prodotti del tipo $\alpha_i\beta_j$, con $i = 1, 2, \ldots, n$ e $j = 1, 2, \ldots, m$, formano una base di F su K e quindi $[F : K] = nm$ come desiderato. Vediamo prima che questi nm vettori *generano* F come spazio vettoriale su K. Sia $y \in F$; allora vale (2) per opportuni $e_j \in E$. Applichiamo (1) ad ogni elemento $e_j \in E$, cioè per ogni $j = 1, 2, \ldots, m$ esistono $k_{ij} \in K$, $i = 1, 2, \ldots, n$, per i quali valgono

$$e_j = \sum_{i=1}^{n} k_{ij}\alpha_i. \tag{3}$$

Sostituendo (3) nell'equazione (2) per y troviamo

$$y = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} k_{ij}\alpha_i \right) \beta_j = \sum_{j=1}^{m} \sum_{i=1}^{n} k_{ij}\alpha_i\beta_j.$$

Per dimostrare che l'insieme $\{\alpha_i\beta_j : i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m\}$ è una base resta da verificare che questi vettori sono linearmente indipendenti. Supponiamo infatti di avere una loro combinazione lineare nulla

$$\sum_{j=1}^{m} \sum_{i=1}^{n} k_{ij}\alpha_i\beta_j = 0.$$

Possiamo scriverla anche come

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} k_{ij}\alpha_i \right) \beta_j = 0,$$

notando che per ogni $j = 1, 2, \ldots, m$ si ha $z_j = \sum_{i=1}^{n} k_{ij}\alpha_i \in E$. Poiché $\beta_1, \ldots, \beta_m$ è una base di F su E, questo è possibile solo se vale $z_j = 0$ per ogni $j = 1, 2, ..., m$. Allora si ha $\sum_{i=1}^{n} k_{ij}\alpha_i = 0$ per $j = 1, 2, \ldots, m$. Poiché $\alpha_1, \ldots, \alpha_n$ è una base di E su K, concludiamo che $k_{ij} = 0$ per ogni $j = 1, 2, ..., m$ e $i = 1, 2, ..., n$. □

12.2 Radici di un polinomio ed estensioni semplici

In questo paragrafo E denota un'estensione del campo K. Se $a \in E$, denotiamo con $K(a)$ il sottocampo di E generato da K e a, cioè il più piccolo sottocampo di E contenente K e a. Più in generale per $a_1, \ldots, a_n \in E$ denotiamo con $K(a_1, \ldots, a_n)$ il sottocampo di E generato da K e $a_1, \ldots, a_n$.

Definizione 12.5. Un'estensione E di K si dice *semplice* se esiste un elemento a di E tale che $E = K(a)$.

Chiaramente $\mathbb{C} = \mathbb{R}(i)$ è un'estensione semplice finita di $\mathbb{R}$. Inoltre si verifica facilmente che il sottoanello $\mathbb{Q}[\sqrt{2}]$ di $\mathbb{R}$ generato da $\mathbb{Q}$ e da $\sqrt{2}$ è un campo, cioè

$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$. Questo dimostra come in certi casi può accadere che l'estensione semplice $K(a)$ risulta essere anche un'estensione semplice di K come estensione di anelli, cioè $K(a) = K[a]$. Per esempio $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$, $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}[\sqrt{5}]$, ma $\mathbb{Q}(\pi) \neq \mathbb{Q}[\pi]$, come vedremo in seguito nell'esempio 12.29. Ciò rende interessante lo studio delle estensioni semplici del tipo $K(a) = K[a]$ alle quali è dedicato questo paragrafo.

Prima di studiare le estensioni semplici in generale, vediamo nel seguente teorema di Kronecker una costruzione concreta di estensioni semplici finite. Essa dipende dalla scelta di un polinomio irriducibile arbitrario $f(x)$ su K. Vedremo nel seguito che tutte le estensioni semplici finite si ottengono in questo modo.

Dalla dimostrazione del teorema di Ruffini 11.43, si evince che il resto della divisione euclidea di $f(x)$ per $x - a$ è esattamente $f(a)$. Possiamo precisare il teorema di Ruffini, introducendo per ogni radice a di $f(x)$ la sua molteplicità.

Definizione 12.6. Sia $f(x) \in K[x]$ e a radice di f. Il massimo $k \in \mathbb{N}$ tale che $(x-a)^k$ divide $f(x)$ si dice *molteplicità* della radice a; è chiaro che $(x-a)^{k+1}$ non divide $f(x)$. La radice a si dice *semplice* se $k = 1$, *multipla* altrimenti.

Si può introdurre la *derivata* $f'(x)$ di un polinomio $f(x) = a_0 + a_1x + \ldots + a_nx^n$ in modo del tutto formale ponendo $f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$. Allora restano valide le usuali proprietà della derivata:

$$(f(x) + g(x))' = f'(x) + g'(x),$$

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x) \quad \text{e} \quad (af(x))' = af'(x)$$

per $f(x), g(x) \in K[x]$ e $a \in K$.

Ora applichiamo il teorema di Ruffini per determinare, in termini della derivata $f'(x)$, quando una radice a di $f(x)$ è multipla.

Lemma 12.7. *Sia K un campo e $f(x) \in K[x]$. Allora una radice α di $f(x)$ è multipla se e solo se α è radice anche della derivata $f'(x)$.*

DIMOSTRAZIONE. Supponiamo che α sia una radice multipla di $f(x)$. Allora

$$(x-\alpha)^2 \text{ divide } f(x),$$

cioè $f(x) = (x-\alpha)^2 g(x)$ per un certo $g(x) \in K[x]$. Pertanto

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$$

e quindi $f'(\alpha) = 0$. Viceversa, se α è radice anche della derivata $f'(x)$, allora dal teorema di Ruffini abbiamo

$$f(x) = (x-\alpha)h(x)$$

per un certo $h(x) \in K[x]$. Ora

$$f'(x) = h(x) + (x-\alpha)h'(x),$$

quindi $f'(\alpha) = 0$ porge $h(\alpha) = 0$. Pertanto il teorema di Ruffini applicato al polinomio $h(x)$ implica $h(x) = (x - \alpha)l(x)$ per un certo $l(x) \in K[x]$. Dunque

$$f(x) = (x - \alpha)^2 l(x).$$

□

Otteniamo anche un altro importante corollario del teorema di Ruffini.

Corollario 12.8. *Siano F e K campi, con $F \geq K$, $f(x) \in K[x]$ polinomio di grado $n > 0$. Allora $f(x)$ ha al più n radici in F contate con la loro molteplicità.*

DIMOSTRAZIONE. Notiamo prima che non è restrittivo supporre $F = K$ poichè la molteplicità di una radice non dipende dal campo dove viene considerata. Procediamo quindi con $F = K$ ragionando per induzione su n. Il caso $n = 1$ è banale. Supponiamo ora $n > 1$ e l'asserto vero per tutti i polinomi di grado $< n$. Sia $\alpha \in K$ una radice di f di molteplicità k. Per il teorema di Ruffini $f(x) = (x - \alpha)^k g(x)$ per qualche $g(x) \in K[x]$ con $g(\alpha) \neq 0$. Quindi le radici di $g(x)$ sono distinte da α e $\deg(g) = n - k < n$. Quindi $g(x)$ ha al più $n - k$ radici in K contate con la loro molteplicità. Di conseguenza $f(x)$ ha al più n radici in K contate con la loro molteplicità. □

Può accadere che f di radici non ne abbia esattamente n o addirittura non ne abbia alcuna. Come prototipi consideriamo i seguenti polinomi a coefficienti nel campo $\mathbb{Q}$ dei numeri razionali:

- $x^2 - 1$, con due radici in $\mathbb{Q}$;
- $x^2 - 2x + 1$, di grado 2 e con una sola radice di molteplicità 2 in qualunque campo;
- $x^2 - 2$, con zero radici in $\mathbb{Q}$, ma due nell'estensione $\mathbb{R}$;
- $x^2 + 1$, con zero radici nel campo reale $\mathbb{R}$ e due nell'estensione $\mathbb{C}$ dei numeri complessi;
- $x^3 - 2$, con zero radici in $\mathbb{Q}$, una sola radice nell'estensione $\mathbb{R}$ e tre nell'estensione $\mathbb{C}$;
- $x^4 - 2$, con zero radici in $\mathbb{Q}$, due nell'estensione $\mathbb{R}$ e quattro nell'estensione $\mathbb{C}$.

Come suggerito da questi esempi, se E è un campo che contiene K (o, in simboli, $K \leq E$), allora si può assumere che $K[x] \subseteq E[x]$ e così f è un polinomio a coefficienti in E. Ci si può domandare se esistono radici di f in E anche se in K non ve ne sono. Il seguente teorema garantisce che esiste sempre un'estensione del campo K in cui f ha radici. Supponiamo dapprima che f sia irriducibile.

Teorema 12.9. (Teorema di Kronecker) *Sia K un campo e $f \in K[x]$ un polinomio irriducibile di grado $n > 0$. Allora esiste un'estensione semplice finita E di K di grado n nella quale $f(x)$ ha una radice α. Risulta inoltre*

$$E = K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}.$$

DIMOSTRAZIONE. Sia $I = (f)$ l'ideale generato da f. Poiché $K[x]$ è dominio principale e $f(x)$ è irriducibile, per il lemma 11.27 e la proposizione 11.30 l'ideale I è massimale. Pertanto il quoziente $K[x]/I$ è un campo per il teorema 9.30. Denotiamo con E il campo $K[x]/I$; sia $\pi : K[x] \to E$ la proiezione canonica. Consideriamo K come sottoanello di $K[x]$ e denotiamo con $j : K \to E$ la restrizione di π a K. Allora j è un omomorfismo non nullo tra i campi K ed E, pertanto j è iniettivo per l'osservazione 10.11. Identifichiamo K con la sua immagine $j(K)$ in E, cioè poniamo $\pi(a) = a$ per ogni $a \in K$. Così E risulta estensione di K. Sia $\alpha = \pi(x) \in E$. Allora $E = K(\alpha)$ e quindi E è un'estensione semplice di K.

Dimostriamo ora che $f(\alpha) = 0$. Infatti, sia $f(x) = b_0 + b_1x + \ldots + b_nx^n$, con $b_0, b_1, \ldots, b_n \in K \subseteq E$. Allora $b_i = \pi(b_i)$ per $i = 1, 2, \ldots, n$, pertanto

$$f(\alpha) = b_0 + b_1\alpha + \ldots + b_n\alpha^n =$$

$$= \pi(b_0) + \pi(b_1)\pi(x) + \ldots + \pi(b_n)\pi(x)^n = \pi(f(x)) = 0.$$

Sia $g(x) \in K[x]$; allora applicando l'algoritmo della divisione euclidea a $g(x)$ e $f(x)$, esistono $q(x), r(x) \in K[x]$ tali che $g(x) = q(x)f(x) + r(x)$, con $r(x) = 0$ oppure $r(x) \neq 0$ e $\deg r < n$. Pertanto se si considera un elemento non nullo $g(x)+I$ in E, si avrà $g(x) + I = r(x) + I$, con $\deg r < n$. Quindi ogni elemento di E si scrive come combinazione lineare a elementi in K di $1, \alpha, \ldots, \alpha^{n-1}$. Per dimostrare che $1, \alpha, \ldots, \alpha^{n-1}$ è una base di E su K, basta ora provare che sono linearmente indipendenti. Supponiamo infatti che esistano $a_0, a_1, ..., a_{n-1} \in K$ tali che

$$0 = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} =$$

$$= \pi(a_0) + \pi(a_1)\pi(x) + \ldots + \pi(a_{n-1})\pi(x)^{n-1} = \pi(g(x)),$$

con $g(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$. Allora $g(x) \in \ker \pi = I = (f)$. Poiché $\deg g < \deg f$, si ha che $g(x)$ è il polinomio nullo, cioè $a_0 = a_1 = ... = a_{n-1} = 0$. Questo dimostra che $1, \alpha, \ldots, \alpha^{n-1}$ è una base di E su K e di conseguenza che il grado $[E : K] = n$. □

Vediamo subito alcune applicazioni di questo teorema.

Esempio 12.10. (a) Sia $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Allora $f(x)$ è irriducibile, essendo di grado 2 e senza radici in $\mathbb{Z}_2$. Il teorema 12.9 assicura che

$$E = \mathbb{Z}_2[x]/(x^2 + x + 1)$$

è un campo di quattro elementi poiché ci sono quattro polinomi $a_0 + a_1x$ di grado ≤ 1 su $\mathbb{Z}_2$.

(b) Sia $f(x)$ un polinomio irriducibile su $\mathbb{Z}_p$ di grado n. Allora $E = \mathbb{Z}_p[x]/(f(x))$ è un campo con p^n elementi.

(c) Per ogni numero primo p esiste un campo con p^2 elementi. Per $p = 2$ l'abbiamo visto in (a). Se $p > 2$, $-1 \neq 1$ in $\mathbb{F}_p$ e d'altro canto $(-1)^2 = 1^2 = 1$. Pertanto l'applicazione $f : \mathbb{F}_p \to \mathbb{F}_p$ definita da $f(a) = a^2$ non è iniettiva. Poiché $\mathbb{F}_p$ è finito, possiamo concludere che f non è nemmeno suriettiva. Esiste quindi un

elemento $b \in \mathbb{F}_p$, tale che $b \neq a^2$ per ogni elemento $a \in \mathbb{F}_p$. Allora il polinomio $f(x) = x^2 - b$ non ha radici in $\mathbb{F}_p$ e quindi è irriducibile. Per il punto (b) il campo $E = \mathbb{Z}_p[x]/(f(x))$ ha p^2 elementi.

Vedremo che l'ipotesi che f sia irriducibile nel teorema 12.9 non è essenziale per quanto riguarda la prima parte del teorema. Infatti:

Corollario 12.11. *Sia K un campo e sia $f \in K[x]$ un polinomio su K. Allora esiste un'estensione semplice E di K dove $f(x)$ ha una radice.*

DIMOSTRAZIONE. Se $f(x)$ è irriducibile si applica il teorema 12.9, altrimenti si scompone $f(x)$ in prodotto di polinomi irriducibili. Sia $g(x)$ uno dei fattori irriducibili di $f(x)$. Allora per il teorema 12.9 esiste un'estensione E di K e una radice $\alpha \in E$ di $g(x)$. Poiché $g(x)$ divide $f(x)$, ovviamente α è radice anche di $f(x)$. □

12.3 Elementi algebrici ed estensioni algebriche

Vedremo che le estensioni costruite nel teorema 12.9 sono *tutte* le estensioni semplici finite. A questo scopo sarà utile la seguente definizione.

Definizione 12.12. Sia $E \geq K$ un'estensione di campi. Un elemento $a \in E$ si dice *algebrico* su K se è radice di un polinomio non nullo $f \in K[x]$. Altrimenti si dice che a è *trascendente* su K. L'estensione $E \geq K$ si dice *algebrica* se tutti gli elementi di E sono algebrici su K.

Dato $\alpha \in E$ si può considerare l'applicazione $\chi_\alpha : K[x] \to E$ definita da $\chi_\alpha(f) = f(\alpha)$ per $f \in K[x]$. Allora χ_α è un omomorfismo di anelli la cui immagine è il sottoanello $K[\alpha]$ di E. Il nucleo $I = \ker \chi_\alpha$ è costituito dai polinomi $f(x) \in K[x]$ tali che $f(\alpha) = 0$. Poiché I è un ideale di $K[x]$ e $K[x]$ è un dominio euclideo (e pertanto a ideali principali), esiste un polinomio $f_{K,\alpha} \in K[x]$ tale che $I = (f_{K,\alpha})$. Inoltre, poiché ogni polinomio è associato ad un polinomio monico grazie al lemma 11.11, possiamo supporre $f_{K,\alpha}$ monico. Osserviamo che deg $f_{K,\alpha}$ è minimo tra tutti i gradi dei polinomi che annullano α. Pertanto α è algebrico su K se e solo se il nucleo I di χ_α è un ideale non nullo. Motivati da queste osservazioni, diamo la seguente definizione.

Definizione 12.13. Dato $\alpha \in E$ elemento algebrico sul campo K, il polinomio $f_{K,\alpha}$ generatore monico del nucleo di χ_α si dice *polinomio minimo di α su K*.

Corollario 12.14. *Sia $\alpha \in E$ un elemento algebrico sul campo K e sia $g(x) \in K[x]$ tale che $g(\alpha) = 0$. Allora il polinomio minimo $f = f_{K,\alpha}$ divide $g(x)$ in $K[x]$.*

DIMOSTRAZIONE. Basta ricordare che il polinomio minimo è il generatore dell'ideale dei polinomi che si annullano in α. □

Dimostriamo innanzitutto che il polinomio minimo è irriducibile.

Lemma 12.15. *Sia $\alpha \in E$ un elemento algebrico sul campo K e $f = f_{K,\alpha}$ il polinomio minimo di α su K Allora f è irriducibile in $K[x]$, l'anello $K[\alpha]$ è un campo e pertanto coincide con $K(\alpha)$ e $[K(\alpha) : K] = \deg f$.*

DIMOSTRAZIONE. Supponiamo che f si scriva come prodotto di g ed h, $f = gh$. Sappiamo che $f(\alpha) = 0$ pertanto sarà ad esempio $g(\alpha) = 0$. Allora

$$g \in \ker \chi_\alpha = (f)$$

e d'altronde $f \in (g)$, da cui segue, per il lemma 11.11, che f e g sono associati. Questo dimostra che f è irriducibile. Poiché $K[x]$ è un dominio principale, segue che l'ideale $I = (f)$ è massimale e quindi $K[x]/(f)$ è un campo. Per il primo teorema di omomorfismo per gli anelli 10.4, si ha che $K[x]/(f) \cong K[\alpha]$. Pertanto l'immagine $K[\alpha]$ di χ_α è un campo che contiene K ed α ed è il più piccolo con tale proprietà, cioè $K[\alpha] = K(\alpha)$. Per il teorema 12.9 si ha che $[K(\alpha) : K] = \deg f$. □

Definizione 12.16. Sia α un elemento algebrico su un campo K. Allora il *grado di α su K* è il grado dell'estensione $[K(\alpha) : K]$.

Possiamo caratterizzare gli elementi algebrici su un campo K come gli elementi che, se aggiunti al campo K, danno luogo ad un'estensione finita.

Corollario 12.17. *Sia E un'estensione del campo K e sia $\alpha \in E$. Allora α è un elemento algebrico su K se e solo se l'estensione semplice $K(\alpha)$ è un'estensione finita di K.*

DIMOSTRAZIONE. Se α è algebrico su K, basta utilizzare il lemma 12.15.

Se $K(\alpha)$ è un'estensione di grado finito n su K, allora i vettori $1, \alpha, \dots, \alpha^n$ sono linearmente dipendenti. Quindi esistono elementi $a_0, a_1, \dots, a_n \in K$, non tutti nulli, tali che $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. Allora α è radice del polinomio non nullo $f(x) = a_0 + a_1x + \dots + a_nx^n$. Pertanto α è algebrico su K. □

Mostriamo ora che le estensioni finite sono algebriche.

Lemma 12.18. *Un'estensione finita è algebrica ed ogni elemento ha grado finito che divide il grado dell'estensione.*

DIMOSTRAZIONE. Supponiamo che E abbia dimensione finita n su K e $\alpha \in E$. Per il teorema 12.4 si ha $[E : K] = [E : K(\alpha)][K(\alpha) : K]$. Allora il grado $[K(\alpha) : K]$ divide n e per il corollario 12.17 in particolare α è algebrico su K. □

Osserviamo che, una volta conosciuto il polinomio minimo $f(x)$ di α su K, siamo in grado di descrivere completamente $K(\alpha)$ tramite il teorema 12.9. In particolare $[K(\alpha) : K]$ è uguale al grado n di f. Gli elementi di K sono tutti e soli quelli di grado 1 su K.

Nel seguente teorema riassumiamo ciò che è stato dimostrato, cioè la caratterizzazione delle estensioni semplici finite, descrivendone gli elementi.

Teorema 12.19. *Sia E/K un'estensione e $\alpha \in E$. Allora sono equivalenti:*

(a) α è algebrico su K con polinomio minimo $f(x) = \sum_{i=0}^{n} \alpha_i x^i$ di grado n;
(b) $[K(\alpha) : K] = n$ è finito;
(c) il sottoanello $K[\alpha] = \{\sum_{i=0}^{n-1} b_i \alpha^i \mid b_i \in K\}$ è un campo, cioè $K(\alpha) = K[\alpha]$;
(d) esistono $b_0, \dots, b_{n-1} \in K$ tali che $\alpha^{-1} = \sum_{i=0}^{n-1} b_i \alpha^i \in K[\alpha]$.

Se queste valgono, esiste un isomorfismo fra $K(\alpha)$ e $K[x]/(f)$, identico su K, dove f è il polinomio minimo di α su K e

$$K(\alpha) = \{g(\alpha) \mid g \in K[x]\} = \left\{ \sum_{i=0}^{n-1} k_i a^i \mid k_i \in K \right\}.$$

DIMOSTRAZIONE. L'equivalenza di (a) e (b) è stata dimostrata nel corollario 12.17. Se vale (a), allora il lemma 12.15 garantisce che $K[\alpha]$ è un campo, cioè vale (c).

(c) implica (d) è ovvia.

Supponiamo ora che valga (d): allora $\alpha^{-1} = \sum_{i=0}^{n-1} b_i \alpha^i \in K[\alpha]$. Moltiplichiamo ambo i membri di questa uguaglianza per α e aggiungiamo -1. Otteniamo così $\sum_{i=0}^{n-1} b_i \alpha^{i+1} - 1 = 0$, da cui α è zero del polinomio $\sum_{i=0}^{n-1} b_i x^{i+1} - 1$, cioè α è algebrico su K. □

Dimostriamo un facile lemma, che sarà utile in diverse dimostrazioni.

Lemma 12.20. *Siano E, F, K campi con $K \leq F \leq E$ e sia $\alpha \in E$ un elemento algebrico su K. Allora α è algebrico su F e vale $[F(\alpha) : F] \leq [K(\alpha) : K]$*

DIMOSTRAZIONE. Per ipotesi α è algebrico su K, quindi esiste un polinomio $f(x)$ in $K[x]$ tale che $f(\alpha) = 0$. Poiché $K \leq F$, si ha $f(x) \in F[x]$; allora il polinomio minimo $g(x)$ di α su F divide $f(x)$. Da questo segue

$$[F(\alpha) : F] = \deg g \leq \deg f = [K(\alpha) : K].$$

□

Dal teorema 12.19 e dal lemma 12.20 otteniamo alcuni importanti risultati.

Lemma 12.21. *Sia E un'estensione del campo K e siano α, β due elementi algebrici di E. Allora anche $\alpha \pm \beta$ e $\alpha\beta$ sono algebrici.*

DIMOSTRAZIONE. Sia $F = K(\alpha)$. Allora F è un'estensione finita di K per il teorema 12.19. Ora β è algebrico su F, quindi l'estensione $F(\beta)$ di F è finita. Per il teorema 12.4 anche l'estensione $F(\beta)$ di K è finita. Quindi per il lemma 12.18 ogni elemento di $F(\beta)$ è algebrico su K; lo sono in particolare $\alpha \pm \beta$ e $\alpha\beta$. □

Da questo lemma segue immediatamente che gli elementi algebrici su un campo formano essi stessi un campo.

Teorema 12.22. *Sia E un'estensione di K. Gli elementi algebrici di E su K formano un sottocampo di E che contiene K.*

DIMOSTRAZIONE. Sia $F = \{\alpha \in E : \alpha$ è algebrico su $K\}$. Allora $K \leq F$, in quanto se $k \in K$, allora k è zero del polinomio $x - k \in K[x]$. Per il lemma 12.21 F è un sottoanello di E. Inoltre se $\alpha \in F$, allora per il teorema 12.19 $\alpha^{-1} \in K(\alpha)$, da cui $[K(\alpha^{-1}) : K] \leq [K(\alpha) : K] < \infty$, cioè $\alpha^{-1} \in F$. □

Dimostriamo ora un altro lemma, che dimostra la transitività della relazione "essere algebrico", definita sulle estensioni di un campo K.

Lemma 12.23. *Siano $K \leq E \leq F$ campi. Se F è algebrico su E e E è algebrico su K, allora F è algebrico su K.*

DIMOSTRAZIONE. Sia $\alpha \in F$; allora esiste un polinomio $f(x) \in E[x]$,

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n, \quad \text{tale che} \quad f(\alpha) = 0.$$

Poiché E è algebrico su K, gli elementi $a_0, \ldots, a_n$ di E sono algebrici su K. Pertanto l'estensione $L = K(a_0, \ldots, a_n)$ è finita su K per il lemma 12.24 e $f(x) \in L[x]$ e quindi α è algebrico su M. Per il teorema dei gradi 12.4 si ha

$$[L(\alpha) : K] = [L(\alpha) : L][L : K] < \infty.$$

Ora $K(\alpha) \leq L(\alpha)$, da cui segue che $[K(\alpha) : K] < \infty$, quindi α è algebrico su K. □

Una caratterizzazione delle estensioni finite è data dal seguente teorema 12.25, a cui facciamo precedere la dimostrazione di una delle due implicazioni, in quanto è interessante di per sé.

Lemma 12.24. *Sia $E = K(\alpha_1, \ldots, \alpha_n)$, con $\alpha_1, \ldots, \alpha_n$ elementi algebrici su K. Allora E/K è finita e pertanto algebrica.*

DIMOSTRAZIONE. Sia $E = K(\alpha_1, \ldots, \alpha_n)$. Facciamo induzione su n. Se $n = 1$, allora per il teorema 12.19 $[K(\alpha) : K]$ è finito. Supponiamo ora $E = K(\alpha_1, \ldots, \alpha_n)$, con $n \geq 2$. Sia $F = K(\alpha_1, \ldots, \alpha_{n-1})$; allora per il teorema dei gradi

$$[E : K] = [E : F][F : K].$$

Osserviamo che $E = F(\alpha_n)$ e per il lemma 12.20 si ha $[E : F] \leq [K(\alpha_n) : K]$, che è finito per ipotesi. Ora $[F : K]$ è finito per ipotesi induttiva e questo conclude la dimostrazione. Il secondo enunciato segue dal lemma 12.18. □

Teorema 12.25. *Un'estensione E di K è finita se e solo se esistono $\alpha_1, ..., \alpha_n$ elementi algebrici su K tali che $E = K(\alpha_1, \ldots, \alpha_n)$.*

DIMOSTRAZIONE. Supponiamo che l'estensione E di K sia finita di grado n. Facciamo induzione su n. Se $n = 1$, allora $E = K = K(1)$. Supponiamo $n \geq 2$ e l'enunciato vero per tutti gli $m < n$. Poiché $n \geq 2$, esiste un elemento $\alpha \in E \setminus K$. Per il lemma 12.18, α è algebrico su K e per il teorema dei gradi, si ha

$$[E : K] = [E : K(\alpha)][K(\alpha) : K].$$

Poiché $[K(\alpha) : K] > 1$, si ha $[E : K(\alpha)] < n$. Applichiamo l'ipotesi induttiva all'estensione E di $K(\alpha)$; allora esistono $\alpha_1, ..., \alpha_r$ algebrici su $K(\alpha)$ tali che

$$E = K(\alpha)(\alpha_1, ..., \alpha_r) = K(\alpha, \alpha_1, ..., \alpha_r)$$

e inoltre $\alpha_1, ..., \alpha_r$ sono algebrici su K per il lemma 12.23.

L'altra implicazione è già stata dimostrata nel lemma 12.24. □

In definitiva le estensioni finite sono tutte e sole quelle algebriche generate da un numero finito di elementi. Quando K è finito o di caratteristica 0 si può dimostrare che $n = 1$, cioè tutte le estensioni finite sono anche semplici. Questo non è vero in generale, come dimostreremo nell'esempio 12.32 nel paragrafo 12.4.

12.4 Estensioni semplici infinite

Il campo dei quozienti del dominio $K[x]$ viene chiamato campo delle *funzioni razionali* di x su K perché ogni elemento di tale campo si rappresenta come quoziente $\frac{f(x)}{g(x)}$ di due polinomi $f(x), g(x) \in K[x]$, con $g(x) \neq 0$. Tale campo si denota con $K(x)$ ed è un'estensione semplice di K *infinita*.

Lemma 12.26. *Se K è un campo, l'anello di polinomi $V = K[x]$ è uno spazio vettoriale sul campo K di dimensione infinita.*

DIMOSTRAZIONE. Supponiamo per assurdo che $\dim V = n$. Allora i vettori $1, x, x^2, \ldots, x^n \in V$ devono essere linearmente dipendenti, quindi esistono elementi non tutti nulli $a_0, a_1, \ldots, a_n \in K$ con $a_0 + a_1x + \ldots + a_nx^n = 0$, assurdo poiché il polinomio $f(x) = a_0 + a_1x + \ldots + a_nx^n$ è non nullo. □

Il seguente teorema caratterizza le estensioni semplici infinite, descrivendone gli elementi. In particolare si vede che ogni estensione semplice infinita di K è isomorfa a $K(x)$.

Teorema 12.27. *Siano E un'estensione del campo K e $a \in E$. Allora sono equivalenti:*

(a) a non è algebrico,

(b) $K(a) = \left\{\frac{g(a)}{h(a)} \mid g, h \in K[x]\ h \neq 0\right\} \cong K(x)$.

In particolare le estensioni di K semplici infinite sono tutte isomorfe al campo delle funzioni razionali sopra il campo K.

DIMOSTRAZIONE. Consideriamo l'omomorfismo di anelli $\chi_a : K[x] \to E$ definito da $\chi_a(f) = f(a)$ per $f \in K[x]$, descritto dopo la definizione 12.12; allora $\ker \chi_a \neq 0$ se e solo se a è algebrico. Pertanto a non è algebrico se e solo se χ_a è un omomorfismo iniettivo con immagine $K[a]$, cioè se e solo se il dominio $K[x]$ è isomorfo al dominio $K[a]$. Supponiamo quindi che a non sia algebrico; allora il

campo dei quozienti $K(a)$ di $K[a]$ è isomorfo al campo dei quozienti $K(x)$ di $K[x]$. Pertanto sono isomorfi anche come spazi vettoriali su K.

Viceversa, se a è algebrico su K, allora per il lemma 12.17 $[K(a) : K]$ è finito, da cui segue che anche $[K(x) : K]$ è finito, in contraddizione con il lemma 12.26. □

Osserviamo che quanto detto per le estensioni semplici trascendenti, non vale in generale per le estensioni semplici algebriche. Infatti estensioni semplici algebriche dello stesso grado non sono necessariamente isomorfe, come dimostra il seguente esempio.

Esempio 12.28. Le estensioni semplici $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ di $\mathbb{Q}$, entrambe di grado 2, non sono isomorfe. Supponiamo infatti che esista un isomorfismo di campi

$$\varphi : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{2}).$$

È facile verificare che $\varphi(a) = a$ per ogni $a \in \mathbb{Q}$ e quindi $\varphi(\sqrt{3}) \notin \mathbb{Q}$ essendo $\sqrt{3} \notin \mathbb{Q}$. Pertanto $\varphi(\sqrt{3}) = a + \sqrt{2}b$ con $a, b \in \mathbb{Q}$ non entrambi nulli. Allora

$$3 = \varphi(3) = \varphi(\sqrt{3}\sqrt{3}) = \varphi(\sqrt{3})\varphi(\sqrt{3}) = (a + \sqrt{2}b)^2 = a^2 + 2b^2 + 2ab\sqrt{2},$$

da cui segue che $\sqrt{2}$ dovrebbe appartenere a $\mathbb{Q}$. Da questa contraddizione discende l'enunciato.

Nel caso speciale delle estensioni $\mathbb{Q} \leq \mathbb{R}$ e $\mathbb{Q} \leq \mathbb{C}$, si usa chiamare un numero reale (complesso) α *numero algebrico* se esso risulta un elemento algebrico di $\mathbb{R}$ (rispettivamente $\mathbb{C}$) su $\mathbb{Q}$, altrimenti α si dice un *numero trascendente.* Secondo un teorema di Cantor di cui omettiamo la facile dimostrazione (si veda l'esercizio 12.49) l'insieme dei numeri algebrici è numerabile. Pertanto la cardinalità dell'insieme dei numeri trascendenti è uguale alla cardinalità di $\mathbb{R}$. Questa dimostrazione indiretta di Cantor che esistono numeri reali trascendenti prescinde delle proprietà intrinseche dei numeri razionali e reali. Liouville sviluppò un altro approccio, basato sull'approssimazione dei numeri reali con numeri razionali, notando che per un numero irrazionale algebrico α l'approssimazione con numeri razionali di α convergono "lentamente", mentre esistono successioni di numeri razionali che convergono "velocemente" e quindi danno luogo ad un numero trascendente.

Esempio 12.29. Charles Hermite (1822 - 1901) dimostrò che il numero

$$e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n$$

è trascendente. Ferdinand von Lindemann (1852-1939) dimostrò che π è trascendente.

Nel seguito useremo il seguente lemma.

Lemma 12.30. *Se K è un campo e $f(x) \in K[x]$ un polinomio irriducibile, allora $f(x)$ ha una radice multipla in qualche estensione E di K se e solo se $f'(x) = 0$.*

DIMOSTRAZIONE. Sia α una radice multipla di $f(x)$ in un'estensione E di K. Allora $f(\alpha) = f'(\alpha) = 0$ e pertanto $x - \alpha$ divide sia $f(x)$ che $f'(x)$. Quindi $x - \alpha$ divide (in $E[x]$) il massimo comun divisore $d(x)$ di $f(x)$ e $f'(x)$. Pertanto $\deg d > 0$. Poiché $f(x), f'(x) \in K[x]$, anche $d(x) \in K[x]$. Di conseguenza $d(x)$ è associato a $f(x)$ in quanto $d(x)|f(x)$ è un divisore di grado positivo e $f(x)$ è irriducibile. Questo implica $f(x)|d(x)$ e quindi $f(x)|f'(x)$. Essendo $\deg f' < \deg f$, questo è possibile solo se $f'(x) = 0$.

Supponiamo ora $f'(x) = 0$. Per l'esercizio 12.48 $\operatorname{char} K = p$ è un numero primo ed esiste un polinomio $g(x) \in K[x]$ tale che $f(x) = g(x^p)$. Sia α una radice di $g(x)$ in qualche estensione di K. Sia E_1 un'estensione di E dove esiste una radice β del polinomio $x^p - \alpha$, cioè $\beta^p = \alpha$. Allora β è una radice di $f(x)$ di molteplicità almeno p. Infatti $g(x) = (x - \alpha)g_1(x)$ per qualche polinomio $g_1(x) \in K[x]$. Quindi si ha $f(x) = g(x^p) = (x^p - \alpha)g_1(x) = (x^p - \beta^p)g_1(x) = (x - \beta)^p g_1(x)$. □

Consideriamo un esempio di un polinomio irriducibile con una radice multipla.

Esempio 12.31. Siano p un numero primo e $K = \mathbb{F}_p(T)$ il campo delle funzioni razionali su $\mathbb{F}_p$. Consideriamo il sottocampo $F = \mathbb{F}_p(T^p)$ di K.

(a) $T \notin F$. Infatti, supponiamo per assurdo di avere $T = \frac{P(T^p)}{Q(T^p)}$, dove P e Q sono polinomi a coefficienti in $\mathbb{F}_p$, diciamo

$$P(T^p) = a_0 + a_1 T^p + \ldots + a_k T^{kp} \quad \text{e} \quad Q(T^p) = b_0 + b_1 T^p + \ldots + b_m T^{mp},$$

con $a_0, a_1, \ldots, a_k, b_0, b_1, \ldots, b_m \in \mathbb{F}_p$, e $a_k \neq 0$, $b_m \neq 0$. Pertanto $\deg P(T^p) = kp$ e $\deg Q(T^p) = mp$. Ora dall'uguaglianza $TQ(T^p) = P(T^p)$ deduciamo che il grado kp di $P(T^p)$ è uguale anche a $mp + 1$, assurdo.

(b) Il polinomio $f(x) = x^p - T^p \in F[x]$ è irriducibile. Infatti, supponiamo per assurdo di avere $f(x) = g(x)h(x)$ con $g(x), h(x) \in F[x]$ e $k = \deg g < p$ positivo. Considerando questa uguaglianza anche in $K[x]$ e tenendo conto dell'uguaglianza $f(x) = (x - T)^p$ valida in $K[x]$, concludiamo $g(x)h(x) = (x - T)^p$ in $K[x]$. Poiché $K[x]$ è un dominio fattoriale, deduciamo che $g(x) = (x - T)^k$ e $h(x) = (x - T)^{p-k}$. Essendo $g(x) = x^k - kTx^{k-1} + \ldots \in F[x]$, abbiamo $kT \in F$. Da $0 < k < p$ si ha $T \in F$, assurdo.

(c) Ora dall'uguaglianza $f(x) = (x - T)^p$ segue che $T \in K$ è una radice di molteplicità p di $f(x)$.

Utilizzando il campo delle funzioni razionali su un campo, costruiamo un esempio di un'estensione finita non semplice.

Esempio 12.32. Sia p un numero primo. Consideriamo come sopra il campo $K = \mathbb{F}_p(x)$ delle funzioni razionali su $\mathbb{F}_p$ ed il campo $E = K(y)$ delle funzioni razionali su K. Consideriamo il sottocampo $F = \mathbb{F}_p(x^p, y^p)$ di E. Si ha che $E = F(x, y)$ e sia x che y sono algebrici su F. Più precisamente x è radice del polinomio irriducibile $f(T) = T^p - x^p \in F[T]$ e y è radice del polinomio irriducibile $g(T) = T^p - y^p \in F[T]$ (ragionare come nel punto (b) dell'esempio 12.31 per verificare l'irriducibilità di questi polinomi). Pertanto le estensioni $F \leq F(x)$ e $F \leq F(y)$ sono entrambe di grado p. Ora vediamo che ogni elemento z di E soddisfa $z^p \in F$. Questo è vero per

$z = x, y$. Essendo E di caratteristica p, questo resta vero anche per tutti i polinomi $f(x,y)$: infatti se a è un coefficiente di $f(x,y)$, $a \in \mathbb{F}_p$, quindi $a^p = a \in \mathbb{F}_p$ e pertanto $f(x,y)^p \in F$, in quanto l'elevamento alla potenza p è un omomorfismo di campi in un campo di caratteristica p. Infine un elemento z arbitrario in E risulta un quoziente

$$f(x,y)/g(x,y) \quad \text{con} \quad f(x,y), g(x,y) \in \mathbb{F}_p[x,y]$$

e ci si riconduce al caso precedente. Ogni elemento z di E soddisfa $z^p \in F$. Dunque l'estensione $F \leq F(z)$ può avere grado al più p. Dato che $[E : F] = p^2$, l'estensione $F \leq E$ non è semplice.

12.5 Campo di spezzamento di un polinomio

Definizione 12.33. Sia $f(x) \in K[x]$ un polinomio monico non costante. Un *campo di spezzamento* di $f(x)$ su K è un'estensione di campi K_f/K tale che:

(1) $f(x)$ si scompone in fattori lineari in $K_f[x]$, cioè $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ con $\alpha_i \in K_f$;
(2) K_f è generato dalle radici di $f(x)$, cioè $K_f = K(\alpha_1, \dots, \alpha_n)$.

L'ultima condizione dice che K_f è la più piccola estensione di K che contiene tutte le radici di $f(x)$. Ora dimostriamo che ogni polinomio ammette un campo di spezzamento.

Teorema 12.34. *Siano K un campo e $f(x) \in K[x]$ un polinomio. Allora esiste un campo di spezzamento K_f di f su K.*

DIMOSTRAZIONE. Proviamo prima che esiste un'estensione E del campo K tale che $f(x)$ si spezza in fattori lineari in $E[x]$. Scriviamo

$$f(x) = g(x)(x - \alpha_1)\dots(x - \alpha_r)$$

dove $\alpha_1, \dots, \alpha_r$ sono elementi del campo K e dove $r \in \mathbb{N}$, quindi r può essere anche 0. Lo dimostriamo per induzione sul grado n di $g(x)$. Se $n = 0$, allora f si spezza in fattori lineari in $K[x]$ e non c'è nulla da provare. Assumiamo quindi $\deg g > 1$; allora per il corollario 12.11 esiste un'estensione F di K in cui $g(x)$ ha uno zero β. Pertanto in $F[x]$ si ha $f(x) = g_0(x)(x - \beta)(x - \alpha_1)\dots(x - \alpha_r)$. Poiché $\deg g_0 < \deg g$, possiamo applicare l'ipotesi induttiva ed ottenere che $f(x)$ si spezza in fattori lineari in una estensione E del campo F, che è anche estensione di K.

Abbiamo visto che esiste un'estensione E di K in cui il polinomio $f(x)$ si spezza in fattori lineari. Si prenda il sottocampo $K_f = K(\alpha_1, \dots, \alpha_n)$ generato dalle sue radici. Questa estensione risulta finita per il teorema 12.25. □

Una conseguenza dell'esistenza di un campo di spezzamento per ogni polinomio su un campo arbitrario, è che, considerando un insieme finito $f_1(x), \dots, f_n(x)$ di polinomi su quel campo, esiste un campo di spezzamento per tutti i polinomi di

quell'insieme finito, cioè un'estensione finita in cui $f_1(x), \ldots, f_n(x)$ si spezzano in fattori lineari.

Ora dimostriamo che il campo di spezzamento di un polinomio a coefficienti in un campo K è unico a meno di isomorfismi che lasciano fissi tutti gli elementi di K.

Teorema 12.35. *Siano K un campo, $f(x) \in K[x]$ e K_f un campo di spezzamento di $f(x)$ su K. Allora per ogni estensione E di K nella quale $f(x)$ si scompone in fattori lineari esiste un omomorfismo di anelli unitari $\varphi : K_f \to E$ tale che $\varphi(a) = a$ per ogni $a \in K$ e $\varphi(\alpha)$ è radice di $f(x)$ in E per ogni radice α di $f(x)$ in K_f.*

DIMOSTRAZIONE. Ragioniamo per induzione sul grado $n = [K_f : K]$. Il caso $n = 1$ è banale. Supponiamo $n > 1$ e l'asserto sia stato dimostrato per tutti i campi K, i polinomi $f(x) \in K[x]$ con $[K_f : K] < n$ e le estensioni E di K in cui $f(x)$ si scompone in fattori lineari. Osserviamo inoltre che se L è un'estensione di K ottenuta aggiungendo a K alcune radici di f, il campo di spezzamento di f su L coincide con K_f.

Supponiamo dapprima che $f(x)$ sia irriducibile e sia α una radice di $f(x)$ in K_f. Poiché per ipotesi $n > 1$, si ha $K < K[\alpha]$. Ora fissiamo una radice arbitraria $\gamma \in E$ di $f(x)$. Ogni elemento $z \in K[\alpha]$ è della forma $z = g(\alpha)$ per qualche $g(x) \in K[x]$. Poniamo $\varphi(z) = g(\gamma)$. Notiamo intanto che $\varphi(a) = a$ per ogni $a \in K$. Se $z = g(\alpha) = h(\alpha)$ con $h(x) \in K[x]$, allora $f(x) | g(x) - h(x)$. Poiché $f(\gamma) = 0$, questo ci permette di concludere che anche $g(\gamma) = h(\gamma)$. Pertanto la definizione di φ è corretta. Per vedere che $\varphi : K[\alpha] \to E$ è un omomorfismo basta notare che se $\xi : K[x] \to E$ e $\zeta : K[x] \to K[\alpha]$ sono gli unici omomorfismi con $\xi(a) = a$ e $\zeta(a) = a$ per ogni $a \in K$ e $\xi(x) = \gamma$ e $\zeta(x) = \alpha$ garantiti dal teorema 11.2, allora $\xi = \varphi \circ \zeta$. L'ultima affermazione segue immediatamente dalla proprietà $\varphi(a) = a$ per ogni $a \in K$. Identifichiamo $K[\alpha]$ con la sua immagine isomorfa $L = \varphi(K[\alpha])$ in E. Si ha che K_f è anche campo di spezzamento di $f(x)$ sull'estensione L di K e $[K_f : L] < [K_f : K] = n$. Quindi per l'ipotesi induttiva applicata al polinomio $f(x) \in L[x]$ e l'estensione E di L esiste un omomorfismo di anelli unitari $\psi : K_f \to E$ tale che $\psi(a) = a$ per ogni $a \in L$ e $\psi(\beta)$ è radice di $f(x)$ in E, per ogni radice β di $f(x)$ in K_f.

Affrontiamo ora il caso generale. Se $f(x)$ è irriducibile, la conclusione segue dal caso considerato sopra. Supponiamo che $f(x) = g(x)h(x)$ con $g(x), h(x) \in K[x]$, $g(x)$ irriducibile con $0 < \deg g < \deg f$. Sia K_g il sottocampo di K_f generato da tutte le radici di $g(x)$ in K_f. Allora K_g è un campo di spezzamento di $g(x)$ su K. Essendo un divisore di $f(x)$, anche $g(x)$ si scompone in fattori lineari in E. Pertanto possiamo applicare il caso già considerato e trovare un omomorfismo di anelli unitari $\varphi : K_g \to E$ tale che $\varphi(a) = a$ per ogni $a \in K$ e $\varphi(\alpha)$ è radice di $g(x)$ in E per ogni radice α di $g(x)$ in K_g. Da ora in poi identificheremo K_g con la sua immagine isomorfa $K_1 = \varphi(K_g)$ in E. Si ha che K_f è anche campo di spezzamento di $f(x)$ sull'estensione K_1 di K e $[K_f : K_1] < [K_f : K] = n$. Quindi per l'ipotesi induttiva applicata al polinomio $f(x) \in K_1[x]$ e l'estensione E di K_1 esiste un omomorfismo di anelli unitari $\psi : K_f \to E$ tale che $\psi(a) = a$ per ogni $a \in K_1$ e $\psi(\alpha)$ è radice di $f(x)$ in E, per ogni radice α di $f(x)$ in K_f. $\square$

Per vedere che il campo di spezzamento di $f(x)$ su K è unico a meno di isomorfismi basta applicare il teorema 12.35 a due campi di spezzamento di $f(x)$ su K.

Proviamo ora un importante fatto sui campi finiti.

Proposizione 12.36. *Sia K un campo finito con $p = \operatorname{char} K$. Allora K ha p^n elementi, dove $n = [K : \mathbb{F}_p]$. Inoltre K coincide con il campo di spezzamento del polinomio $x^{p^n} - x$ su $\mathbb{F}_p$.*

DIMOSTRAZIONE. Il sottocampo fondamentale di K deve essere un campo finito e pertanto deve essere isomorfo a $\mathbb{F}_p$ per qualche primo p, da cui $p = \operatorname{char} K$. L'uguaglianza $|K| = q = p^n$ segue dalla definizione del grado $[K : \mathbb{F}_p]$. Ora ogni elemento di K è radice del *polinomio fondamentale* $f(x) = x^q - x$ di K. Infatti se $k = 0$, banalmente $0^q = 0$. Se $k \neq 0$, allora k è un elemento del gruppo moltiplicativo $(K^*, \cdot)$. Come abbiamo dimostrato nel corollario 5.54 $k^m = 1$, se $m = |K^*| = q - 1$. Da questo ricaviamo $k^q = k$ e di conseguenza $k^{p^n} = k$ per ogni $k \in K$. Pertanto K è esattamente l'insieme delle radici di $f(x)$ ed è quindi campo di spezzamento di f su ogni suo sottocampo, in particolare sul suo sottocampo fondamentale $\mathbb{F}_p$. □

Vediamo alcuni esempi, altri se ne troveranno nel paragrafo degli esercizi.

Esempio 12.37. In questo esempio vogliamo chiarire quando un campo finito F_1 di cardinalità p^n è contenuto in un altro campo finito F_2 di cardinalità p^m. Dimostreremo che $F_1 \subseteq F_2$ se e solo se $n|m$.

Per impostare correttamente il problema consideriamo un'estensione E del campo finito $\mathbb{F}_p$ che contenga sia il campo F_1 che il campo F_2. Supponiamo che $F_1 \subseteq F_2$ e sia d il grado $[F_2 : F_1]$. Allora $p^m = |F_2| = |F_1|^d = (p^n)^d = p^{nd}$. Quindi $m = nd$ e pertanto $n|m$.

Ora supponiamo che $n|m$ e ricordiamo che F_1 può essere considerato come il campo di spezzamento del polinomio $f(x) = x^{p^n} - x$. Pertanto ogni $\alpha \in F_1$ è radice del polinomio $f(x)$, ovvero $\alpha^{p^n} = \alpha$. Da qui ricaviamo per induzione su d che $\alpha^{p^{nd}} = \alpha$ per ogni d. In particolare $\alpha^{p^m} = \alpha$ poiché $n|m$. In altre parole, α è radice anche del polinomio $g(x) = x^{p^m} - x$. Poiché il sottocampo F_2 di E contiene p^m radici distinte di $g(x)$ e questo polinomio non può avere più di p^m radici in E, concludiamo che α coincide con una di queste radici e quindi $\alpha \in F_2$.

Esempio 12.38. (a) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ è un'estensione di grado 2, perché $\mathbb{Q}(\sqrt{2})$ è il campo di spezzamento del polinomio $f(x) = x^2 - 2$ su $\mathbb{Q}$.
(b) Il campo $\mathbb{Q}(\sqrt[3]{5})$ non è il campo di spezzamento di $f(x) = x^3 - 5$ su $\mathbb{Q}$. Infatti il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt[3]{5}, \omega)$, dove $\omega = -1/2 + i\sqrt{3}/2$ è una radice cubica dell'unità.

12.6 Campi algebricamente chiusi

In questo paragrafo ci dedicheremo allo studio di una classe di campi K per i quali i polinomi irriducibili su K sono della forma più semplice possibile, cioè lineari.

Definizione 12.39. Un campo K si dice *algebricamente chiuso* se ogni polinomio di grado > 0 ha almeno una radice in K.

Teorema 12.40. *Un campo K è algebricamente chiuso se e solo se ogni polinomio di grado > 0 su K si fattorizza in prodotto di fattori lineari.*

DIMOSTRAZIONE. La condizione del teorema implica che il campo K è algebricamente chiuso. Supponiamo ora che K sia algebricamente chiuso e sia $f(x)$ un polinomio di grado $n > 0$. Dimostriamo per induzione su n che $f(x)$ si fattorizza in prodotto di fattori lineari. Se $n = 1$, questo è banalmente vero. Supponiamo $n > 1$ e l'asserto vero per $n - 1$. Per ipotesi $f(x)$ ha una radice $\alpha \in K$. Per il teorema di Ruffini $f(x) = (x - \alpha)g(x)$, dove $g(x) \in K[x]$. Si ha deg $g(x) = n - 1$, quindi $g(x)$ si fattorizza in prodotto di fattori lineari per l'ipotesi induttiva. Questo dimostra il teorema. □

Enunciamo senza dimostrarlo il seguente teorema che assicura l'esistenza di sufficienti campi algebricamente chiusi.

Teorema 12.41. *Sia K un campo arbitrario. Allora esiste un'estensione $E \geq K$ con le seguenti proprietà:*

(1) E è un'estensione algebrica di K;
(2) il campo E è algebricamente chiuso.

Il *teorema fondamentale dell'algebra* garantisce che il campo dei numeri complessi $\mathbb{C}$ è algebricamente chiuso.

La dimostrazione del teorema fondamentale dell'algebra 12.44 che daremo è basata sui seguenti due teoremi.

Teorema 12.42. (Teorema di Cauchy del minimo) *Per ogni polinomio $f(x) \in \mathbb{C}[x]$ esiste $c \in \mathbb{C}$ con*

$$|f(c)| = \inf\{|f(z)| : z \in \mathbb{C}\}. \tag{4}$$

DIMOSTRAZIONE. Sia $f(x) = a_0 + \ldots + a_n x^n$ e siano $n \geq 1$ e $a_n \neq 0$. Dimostreremo prima che

$$\text{esiste } r \in \mathbb{R} \text{ tale che } |f(z)| > |f(0)| \text{ per tutti gli } z \in \mathbb{C} \text{ con } |z| > r. \tag{5}$$

Per $z \neq 0$ abbiamo $|f(z)| = |z|^n \cdot |a_n + h(z^{-1})|$, dove h è il polinomio

$$h(y) = a_{n-1}y + \ldots + a_0 y^n.$$

Poiché $|h|$ è continua per $y = 0$ e $h(0) = 0$ e $a_n \neq 0$, esiste $\delta > 0$ tale che

$$|h(z)| \leq \frac{1}{2}|a_n|$$

per $|z| < \delta$. Allora

$$|f(z)| \geq |z|^n \cdot (|a_n| - |h(z^{-1})|) \geq \frac{1}{2}|a_n| \cdot |z|^n$$

quando $|z| > \delta^{-1}$. Adesso basta scegliere r con $r > \delta^{-1}$ e $|a_n| \cdot r^n > 2 \cdot |f(0)|$ per avere (5).

Sia $C_r = \{z \in \mathbb{C} : |z| \leq r\}$ il cerchio chiuso di centro 0 e raggio r in $\mathbb{C}$. Poniamo $a = \inf\{|f(z)| : z \in C_r\}$. Allora esiste una successione (z_m) di numeri complessi con

$$|z_m| \leq r \text{ per tutti gli } m \in \mathbb{N} \text{ e } \lim_m f(z_m) = a. \tag{6}$$

Siano $r_m = |z_m|$ e φ_m l'argomento di z_m con $\varphi_m \in [0, 2\pi]$. Allora esiste una successione strettamente crescente di indici (m_k) tale che le sottosuccessioni (r_{m_k}) e (φ_{m_k}) siano convergenti in $\mathbb{R}$, con $r_0 = \lim_k r_{m_k}$ e $\varphi_0 = \lim_k \varphi_{m_k}$. Osserviamo che $r_0 \geq 0$ e $\varphi_0 \in [0, 2\pi]$. Poniamo $c = r_0(\cos\varphi_0 + i \sin\varphi_0)$. Allora la successione z_{m_k} converge a c e quindi

$$\lim_k |z_{m_k} - c| = 0. \tag{7}$$

Per il teorma di Ruffini esiste un polinomio $g(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$ tale che $f(x) - f(c) = (x - c)g(x)$. Allora

$$|g(z)| \leq |b_0| + |b_1|r^2 + \ldots + |b_{n-1}|r^{n-1} = A,$$

per tutti gli $z \in C_r$. Quindi $|f(z_{m_k}) - f(c)| = |z_{m_k} - c||g(z)| \leq A|z_{m_k} - c|$ converge a 0 per (7). Da (6) troviamo

$$f(c) = a = \min\{|f(z)| : z \in C_r\}.$$

Poiché $|f(c)| \leq |f(0)| \leq \inf\{|f(z)| : z \in \mathbb{C} \setminus C_r\}$ per (5), segue (4). □

Il fatto che esista $c \in C_r$ con $|f(c)| = \min\{|f(z)| : z \in C_r\}$ segue direttamente anche dal teorema di Weierstrass: ogni funzione continua sul cerchio chiuso C_r a valori in $\mathbb{R}$ assume il suo massimo e minimo su C_r. Nel caso della funzione $|f(x)|$ abbiamo dato una dimostrazione diretta per evitare il ricorso al teorema di Weierstrass.

Faremo anche uso della disuguaglianza di Argand, di cui riportiamo la dimostrazione nel seguente teorema 12.43.

Teorema 12.43. (Disuguaglianza di Argand) *Sia $f(x) \in \mathbb{C}[x]$ un polinomio non costante e sia $c \in \mathbb{C}$ con $f(c) \neq 0$. Allora esiste $c' \in \mathbb{C}$ con $|f(c')| < |f(c)|$.*

DIMOSTRAZIONE. Poniamo $h(x) = (f(c))^{-1} f(c + x)$, allora $h(x)$ ha termine noto 1 e quindi

$$h(x) = 1 + b_k x^k + b_{k+1} x^{k+1} + \ldots + b_n x^n \text{ con } 1 \leq k \leq n \text{ e } b_k \in \mathbb{C}^*.$$

Sia a una radice k-esima di $-1/b_k$, cioè

$$a^k b_k = -1. \tag{8}$$

Allora per il polinomio $g(x) = b_{k+1}x + \ldots + b_n x^{n-k}$, tenuto conto di (8) e osservando che $h(x) = 1 + x^k(b_k + g(x))$, si ha

$$h(at) = 1 - t^k + t^k a^k g(at) \text{ per ogni } t \in]0,1[.$$

Quindi
$$|h(at)| \leq |1 - t^k| + |t^k a^k g(at)| = 1 - t^k + |t^k a^k g(at)|.$$

Per la continuità della funzione $r(t) = a^k g(at)$ in 0 ed essendo $r(0) = 0$, esiste $\delta \in \mathbb{R}$, $\delta > 0$ tale che $|a^k g(at)| < 1/2$ per ogni $t \in (0, \delta)$. Allora con $u = \delta a/2$ abbiamo
$$|h(u)| \leq 1 - t^k + 1/2t^k < 1. \tag{9}$$

Ora, con $c' = c + u$, la disuguaglianza (9) e la definizione di $h(x)$ porgono $|f(c')| = |h(u)| \cdot |f(c)| < |f(c)|$. □

Teorema 12.44. (Teorema fondamentale dell'algebra) *Il campo $\mathbb{C}$ è algebricamente chiuso.*

DIMOSTRAZIONE. Sia $f(x) \in \mathbb{C}[x]$. Applichiamo il teorema di Cauchy del minimo per trovare $c \in \mathbb{C}$ soddisfacente (4). Supponiamo per assurdo $f(c) \neq 0$. Allora per la disuguaglianza di Argand esiste $c' \in \mathbb{C}$ con $|f(c')| < |f(c)|$, che contraddice (4). □

Questo teorema risolve completamente la questione della fattorizzazione dei polinomi su $\mathbb{R}$.

Teorema 12.45. *I polinomi irriducibili di $\mathbb{R}[x]$ sono i polinomi di grado 1 e i polinomi $x^2 + px + q$ di grado 2 con $\Delta = p^2 - 4q < 0$.*

DIMOSTRAZIONE. Sia $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{R}[x]$. Allora $f(x)$ appartiene anche a $\mathbb{C}[x]$ e quindi per il teorema 12.40 $f(x)$ si fattorizza in prodotto di fattori lineari su $\mathbb{C}$ perché $\mathbb{C}$ è algebricamente chiuso. Possiamo assumere che $f(x)$ sia monico. Siano $z_1, z_2, \ldots, z_n$ tutte le radici complesse di $f(x)$. Allora

$$f(x) = (x - z_1)(x - z_2)\ldots(x - z_n).$$

Poiché i coefficienti di f sono reali, per ogni radice $z \in \mathbb{C}$ di $f(x)$ anche $\overline{z}$ è radice di $f(x)$. Infatti

$$f(\overline{z}) = a_0 + a_1\overline{z} + \ldots + a_n\overline{z}^n = \overline{a}_0 + \overline{a}_1\overline{z} + \ldots + \overline{a}_n\overline{z}^n =$$
$$= \overline{a_0 + a_1z + \ldots + a_nz^n} = \overline{f(z)} = 0.$$

Siano $z_1, z_2, \ldots, z_r$ tutte le radici reali di $f(x)$, allora $n - r = 2m$ è un numero pari e le altre radici si possono raggruppare in m coppie di radici

$$z_i, \overline{z}_i, \quad \text{con } i = r+1, \ldots, r+m.$$

Il prodotto $(x - z_i)(x - \overline{z}_i)$ porge

$$(x - z_i)(x - \overline{z}_i) = x^2 - (z_i + \overline{z}_i)x + z_i\overline{z}_i = x^2 + p_ix + q_i,$$

dove $p_i = z_i + \overline{z}_i = 2Re(z_i)$ e $q_i = z_i\overline{z}_i = |z_i|^2$ sono numeri reali. Quindi

$$f(x) = (x - z_1)\dots(x - z_r)(x^2 + p_{r+1}x + q_{r+1})\dots(x^2 + p_{r+m}x + q_{r+m}). \quad (10)$$

Dunque ogni polinomio $f(x) \in \mathbb{R}[x]$ si fattorizza in prodotto di fattori lineari e fattori di secondo grado come in (10). Un polinomio $x^2 + px + q \in \mathbb{R}[x]$ è irriducibile su $\mathbb{R}$, cioè non ha radici in $\mathbb{R}$, se e solo se $\Delta = p^2 - 4q < 0$. □

Teorema 12.46. *Per ogni primo p esiste un'estensione algebrica e algebricamente chiusa* $\mathbb{F}_{p^\infty}$ *di* $\mathbb{F}_p$.

DIMOSTRAZIONE. Per ogni $n \in \mathbb{N}$ poniamo $E_n = \mathbb{F}_{p^{n!}}$. Poiché $n!$ divide $(n+1)!$ per ogni n, segue dall'esempio 12.37 che E_{n+1} è estensione di E_n per ogni n. Nell'unione $E = \bigcup_n E_n$ introduciamo facilmente le operazioni + e $\cdot$ usando il fatto che per ogni coppia $x, y \in E$ esiste n tale che $x, y \in E_n$, pertanto $x + y$ e $x \cdot y$ sono già definiti in E_n. Usando il fatto che ogni terna di elementi a, b e c di E è contenuta in qualche campo E_n, si verifica immediatamente che con queste operazioni E risulta un campo. Inoltre l'estensione $\mathbb{F}_p \subseteq E$ è algebrica essendo ogni elemento $a \in E$ contenuto in un'estensione $\mathbb{F}_p \subseteq E_n$ finita, e quindi algebrica. Sia ora $f(x) \in E[x]$. Allora esiste n tale che $f(x) \in E_n[x]$. Chiaramente $f(x)$ ha una radice α in un'estensione finita K di E_n. Ma allora K è un campo finito in quanto estensione finita di un campo finito. Sia $|K| = p^k$. Allora esiste $m \geq n$ tale che $k|m!$, e quindi K è isomorfo ad un sottocampo di E_m. Essendo K un campo di spezzamento del polinomio $x^{p^k} - x$ e E_m un campo che contiene una copia isomorfa di K, $f(x)$ ha sicuramente radici (infatti, p^k radici) in E. □

Ragionando analogamente, per ogni campo numerabile K si può costruire una estensione algebrica e algebricamente chiusa E di K in due passi. Prima si costruisce un'estensione numerabile F di K dove tutti i polinomi di $K[x]$ hanno una radice. A questo scopo elenchiamo $\{f_n(x) : n \in \mathbb{N}_+\}$ tutti i polinomi di $K[x]$. Definiamo le estensioni F_n per induzione come segue: $F_0 = K$ e per $n > 0$ F_n denoterà il campo di spezzamento di f_n su K_{n-1}. Denotiamo con F l'unione $\bigcup_n F_n$ e la rendiamo un campo some sopra. Non è difficile vedere che tutti i polinomi di $K[x]$ hanno una radice in F e F è numerabile. Adesso costruiamo una successione di estensioni E_n di F, ponendo $E_0 = F$ e per $n > 0$ si costruisce E_n come estensione del campo numerabile E_{n-1} in modo tale che ogni polinomio su E_{n-1} abbia una radice in E_n. Poniamo $E = \bigcup_n E_n$ e lo rendiamo un campo come prima. La verifica che E è un'estensione algebrica e algebricamente chiusa E di K è immediata.

12.7 Polinomi ciclotomici su $\mathbb{Q}$

In questo paragrafo prendiamo in considerazione i polinomi ciclotomici su $\mathbb{Q}$ e dimostriamo che sono irriducibili. Essi vengono definiti come segue.

Definizione 12.47. Sia ξ una radice n-esima di 1 in $\mathbb{C}$ e cioè $\xi \in \mathbb{C}$ e $\xi^n = 1$. Allora ξ si dice *radice primitiva* se $\xi^k \neq 1$ per ogni k tale che $1 \leq k < n$.

Definizione 12.48. Dicesi *n-esimo polinomio ciclotomico* su $\mathbb{Q}$ il polinomio monic $\Phi_n(x)$ avente come radici tutte e sole le radici primitive n-esime di 1 nel campo dei numeri complessi.

Si può dimostrare che il numero delle radici n-esime primitive dell'unità è pa al numero $\varphi(n)$ degli interi positivi minori di n e con esso coprimi (esercizio 12.25

Osserviamo che $\Phi_n(x) = (x - \xi_1)...(x - \xi_{\varphi(n)})$ è un polinomio monico. Dimo streremo, per induzione, che $\Phi_n(x) \in \mathbb{Z}[x]$ per ogni $n \in \mathbb{N}$. A questo scopo avrem bisogno del seguente lemma.

Lemma 12.49. *Per ogni* $n \in \mathbb{N}$ *si ha*

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \qquad (11$$

DIMOSTRAZIONE. Sia ξ una radice n-esima di 1 in $\mathbb{C}$ e d il suo periodo, considerat ξ come elemento del gruppo moltiplicativo delle radici di 1 in $\mathbb{C}$. Allora ξ sarà radic primitiva d-esima di 1 e pertanto sarà radice di $\Phi_d(x)$. D'altra parte, per due diviso distinti d, d' di n, i polinomi $\Phi_d(x)$ e $\Phi_{d'}(x)$ non hanno radici comuni, mentre ogn radice di $\Phi_d(x)$ è anche una radice di $x^n - 1$. Questo dimostra che entrambi i pol nomi in (11) hanno le stesse radici, che risultano tutte semplici. Essendo entrambi polinomi monici, possiamo dedurre che coincidono. □

È facile vedere che

$$\Phi_2(x) = x + 1, \qquad \Phi_3(x) = x^2 + x + 1, \qquad \Phi_4(x) = x^2 + 1,$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \qquad \Phi_6(x) = x^2 - x + 1,$$

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \qquad \Phi_8(x) = x^4 + 1.$$

Teorema 12.50. *Il polinomio* $\Phi_n(x) \in \mathbb{Z}[x]$ *per ogni* $n \in \mathbb{N}$.

DIMOSTRAZIONE. Sia K il campo di spezzamento del polinomio $x^n - 1$. Chiaramen te $\Phi_n(x) \in K[x]$. Dimostriamo per induzione che $\Phi_n(x) \in \mathbb{Z}[x]$ per ogni $n \in \mathbb{N}$. Pe $\Phi_1(x) = x - 1$ questo è ovvio. Supponiamo ora $n > 1$ e $\Phi_k(x) \in \mathbb{Z}[x]$ per tutti i k co $1 \leq k < n$. Dalla formula (11) del lemma 12.49 si vede che $\Phi_n(x) = (x^n - 1)/g(x$ dove $g(x) = \prod_{d|n, d<n} \Phi_d(x)$. Per l'ipotesi induttiva, $g(x) \in \mathbb{Z}[x]$. Poiché $g(x)$ anche monico e $x^n - 1 \in \mathbb{Z}[x]$, concludiamo che anche il polinomio $\Phi_n(x) \in K[x$ ottenuto tramite la divisione di $x^n - 1$ per $g(x)$ in $K[x]$, deve avere tutti i suo coefficienti in $\mathbb{Z}[x]$. □

Poiché i polinomi $\Phi_n(x)$ sono monici, l'irriducibilità su $\mathbb{Z}$ è equivalente a que la su $\mathbb{Q}$, grazie al teorema 11.54. Per dimostrare che i polinomi ciclotomici son irriducibili su $\mathbb{Z}$ necessitiamo di alcuni lemmi.

Definizione 12.51. Un numero complesso α si dice un numero algebrico *intero* s esiste un polinomio monico $f(x) \in \mathbb{Z}[x]$ con radice α.

Le radici dell'unità sono dei numeri algebrici interi. Ora vediamo che il polinomio minimo di un numero algebrico intero ha coefficienti interi.

Lemma 12.52. *Sia $\alpha \in \mathbb{C}$ un numero algebrico intero e sia $p(x)$ il suo polinomio minimo su $\mathbb{Q}$. Allora $p(x) \in \mathbb{Z}[x]$ e divide, in $\mathbb{Z}[x]$, ogni polinomio $h(x) \in \mathbb{Z}[x]$ con $h(\alpha) = 0$.*

DIMOSTRAZIONE. Sia $h(x) \in \mathbb{Z}[x]$ un polinomio monico con radice α ed $f(x)$ in $\mathbb{Z}[x]$ il polinomio primitivo associato a $p(x)$. Allora $p(x)$ divide $h(x)$ in $\mathbb{Q}[x]$ e quindi anche $f(x)$ divide $h(x)$ in $\mathbb{Q}[x]$. Di conseguenza

$$h(x) = f(x)G(x)$$

con $G(x) \in \mathbb{Z}[x]$ per il lemma 11.53. Poichè $h(x)$ è monico, concludiamo che il coefficiente direttivo di $f(x)$ è ± 1, quindi $f(x) = \pm p(x)$ poichè $p(x)$ è monico. Questo dimostra che $p(x) \in \mathbb{Z}[x]$. Abbiamo già visto che $p(x)$ divide $h(x)$ in $\mathbb{Q}[x]$ e dunque, per il lemma 11.53, lo divide anche in $\mathbb{Z}[x]$. □

Teorema 12.53. *I polinomi ciclotomici $\Phi_n(x)$ sono irriducibili su $\mathbb{Z}$.*

DIMOSTRAZIONE. Sia α una radice primitiva n-esima di 1, cioè $\Phi_n(\alpha) = 0$. Sia $f(x) \in \mathbb{Q}[x]$ il polinomio minimo di α. Allora $f(x) \in \mathbb{Z}[x]$ per il lemma 12.52 ed è quindi un polinomio primitivo. Sempre per lo stesso lemma, $f(x)$ divide $\Phi_n(x)$ in $\mathbb{Z}[x]$ e quindi

$$\Phi_n(x) = f(x)G(x) \tag{12}$$

per qualche $G(x) \in \mathbb{Z}[x]$. Osserviamo che $f(x)$, essendo primitivo e irriducibile in $\mathbb{Q}[x]$ è irriducibile anche in $\mathbb{Z}[x]$ per il teorema 11.54. Allora basterà dimostrare che $\Phi_n(x) = \pm f(x)$. A questo scopo basta vedere che anche $\Phi_n(x)$ divide $f(x)$. Per questo proveremo che tutte le radici di $\Phi_n(x)$ sono anche radici di $f(x)$.

Le radici di $\Phi_n(x)$ sono della forma α^k con $1 \leq k < n$ e k coprimo con n. Quindi $k = p_1 \cdot \ldots \cdot p_s$, dove i p_i sono numeri primi coprimi con n. Proviamo che se ξ è una radice comune di $\Phi_n(x)$ e $f(x)$, allora per ogni primo p coprimo con n anche ξ^p è radice di $f(x)$. Supponiamo per assurdo che ciò non accada. Allora esiste $\xi \in \mathbb{C}$ con $\Phi_n(\xi) = f(\xi) = 0$ e $f(\xi^p) \neq 0$. Poiché il primo p non divide n, avremo anche $\Phi_n(\xi^p) = 0$ come già notato sopra. Dalla nostra ipotesi e (12) risulta $G(\xi^p) = 0$. Allora, con $H(x) = G(x^p) \in \mathbb{Z}[x]$, si ha $H(\xi) = 0$, e quindi $f(x)$ divide $H(x)$ per il lemma 12.52. Sia

$$H(x) = f(x) \cdot g(x) \quad \text{in} \quad \mathbb{Z}[x].$$

Proiettando su $\mathbb{F}_p[x]$ si ha

$$\overline{H}(x) = \overline{f}(x) \cdot \overline{g}(x).$$

D'altra parte

$$\overline{H}(x) = \overline{G}(x^p) = (\overline{G}(x))^p = \overline{f}(x) \cdot \overline{g}(x),$$

la seconda uguaglianza dovuta al fatto che $\mathbb{F}_p$ ha caratteristica p. Sia $\psi(x) \in \mathbb{F}_p[x]$ un divisore irriducibile di $\overline{f}(x)$. Allora $\psi(x)$ divide anche $(\overline{G}(x))^p$ e quindi anche $\overline{G}(x)$. Ora (12) porge

$$\overline{\Phi}_n(x) = \overline{f}(x) \cdot \overline{G}(x),$$

e quindi $(\psi(x))^2$ divide $\overline{\Phi}_n(x)$. Poiché $\Phi_n(x)$ divide $x^n - 1$ in $\mathbb{Z}[x]$ per il lemma 12.52, proiettando su $\mathbb{F}_p[x]$ si ha che $\overline{\Phi}_n(x)$ divide $x^n - 1$ in $\mathbb{F}_p[x]$. Quindi $(\psi(x))^2$ divide $x^n - 1$ in $\mathbb{F}_p[x]$. Allora $\psi(x)$ divide anche la derivata nx^{n-1} di $x^n - 1$ per il lemma 12.7. Poiché i polinomi nx^{n-1} e $x^n - 1$ sono coprimi in $\mathbb{F}_p[x]$, perché p non divide n, questo è assurdo. Quindi $f(\xi^p) = 0$.

Sia ora $\beta = \alpha^k$ una radice di $\Phi_n(x)$. Allora $\beta = \alpha^{p_1 \cdots p_s}$ con p_i numeri primi e $(p_i, n) = 1$ per ogni $i = 1, ..., s$. Dimostriamo che β è radice di $f(x)$ per induzione su s. Il caso $s = 1$ lo abbiamo appena dimostrato. Sia $s > 1$ e $\xi = \alpha^{p_1 \cdots p_{s-1}}$, allora ξ è zero di $f(x)$ per ipotesi induttiva, quindi nuovamente per il caso $s = 1$ si ha che $\xi^{p_s} = \beta$ è radice di $f(x)$. Questo conclude la dimostrazione. □

Osserviamo che il caso in cui n sia un primo era già stato dimostrato nell'esempio 11.59, utilizzando il criterio di Eisenstein.

12.8 Polinomi su campi finiti

Osserviamo che il campo di spezzamento del polinomio $x^p - x$ definito sul campo finito $\mathbb{F}_p$, p primo, è $\mathbb{F}_p$ stesso. Ricordiamo che l'elevamento alla potenza p su un campo di caratteristica p è un omomorfismo di campo.

Teorema 12.54. *Se K è un campo finito e $f(x) \in K[x]$ un polinomio irriducibile, allora $f(x)$ ha solo radici semplici in qualsiasi estensione E di K.*

DIMOSTRAZIONE. Infatti se α fosse una radice multipla di $f(x)$ in un'estensione E di K, allora risulterebbe $f'(x) = 0$ per il lemma 12.30. Per l'esercizio 12.48 esiste un polinomio $g(x) \in K[x]$ tale che $f(x) = (g(x))^p$, assurdo, essendo $f(x)$ irriducibile. □

Vediamo ora i polinomi di Artin che definiamo dapprima sul campo finito $\mathbb{F}_p$.

Definizione 12.55. Sia p un numero primo. Dicesi *polinomio di Artin* su $\mathbb{F}_p$ un polinomio del tipo

$$f_a(x) = x^p - x + a,$$

dove a è un elemento non nullo di $\mathbb{F}_p$.

Dimostriamo che i polinomi di Artin sono irriducibili su $\mathbb{F}_p$.

Teorema 12.56. *Sia p un numero primo e $a \in \mathbb{F}_p$ diverso da 0. Allora il polinomio di Artin $f_a(x)$ è irriducibile su $\mathbb{F}_p$.*

DIMOSTRAZIONE. Sia $d(x)$ un divisore monico di $f_a(x) = x^p - x + a$ nell'a dei polinomi $\mathbb{F}_p[x]$ di grado $s = \deg d > 0$. Dimostreremo che $s = p$ e q ır $d(x) \sim f_a(x)$.

Sia E il campo di spezzamento di $f_a(x)$ e sia $\alpha \in E$ una radice di $f_a(x)$. anche $\alpha + k$ è una radice di $f_a(x)$ per tutti i $k \in \mathbb{F}_p$. Infatti

$$f_a(\alpha+k) = (\alpha+k)^p-(\alpha+k)+a = \alpha^p+k^p-\alpha-k+a = \alpha^p-\alpha+a = f_a(\alpha) = 0.$$

Poiché $\alpha, \alpha+1, \ldots, \alpha+(p-1)$ sono p radici diverse di $f_a(x)$ e $\deg f_a = p$, queste sono *tutte* le radici di $f_a(x)$. Poiché il polinomio $d(x)$ divide $f_a(x)$ le radici di $d(x)$ sono $x_1 = \alpha + k_1, x_2 = \alpha + k_2, \ldots, x_s = \alpha + k_s$, con $k_1, k_2, \ldots, k_s \in \mathbb{F}_p$. Pertanto

$$d(x) = (x-x_1)(x-x_2)\ldots(x-x_s) = x^s - (x_1 + x_2 + \ldots + x_s)x^{s-1} + \ldots.$$

Allora, con $b = k_1 + k_2 + \ldots + k_s$, si ha $\sum_{i=1}^{s} x_i = s\alpha + b = c \in \mathbb{F}_p$ poiché tutti i coefficienti di $d(x)$ sono in $\mathbb{F}_p$. Ora $\alpha \notin \mathbb{F}_p$ e $p \geq s > 0$ implicano $s = p$, altrimenti s sarebbe invertibile in $\mathbb{F}_p$ e pertanto $\alpha = s^{-1}(c-b) \in \mathbb{F}_p$. □

Introduciamo i polinomi di Artin su $\mathbb{Z}$.

Definizione 12.57. Un polinomio $f(x) \in \mathbb{Z}[x]$ di grado un primo p e tale che la p-proiezione $\overline{f}(x) \in \mathbb{F}_p[x]$ sia polinomio di Artin su $\mathbb{F}_p$ si dice *polinomio di Artin* su $\mathbb{Z}$.

Per esempio un polinomio $f(x) \in \mathbb{Z}[x]$ del tipo $f(x) = x^p - x + k$, è un polinomio di Artin su $\mathbb{Z}$, se p è un numero primo e k è un numero intero coprimo con p essendo $\overline{f}(x) = f_a$, dove $a = [k]_p \in \mathbb{F}_p$ è il resto di k modulo p. Questo polinomio è anche monico, e quindi primitivo, ma in generale un polinomio di Artin su $\mathbb{Z}$ può non essere primitivo, si veda l'esercizio 12.16 per un esempio.

Lemma 12.58. *I polinomi di Artin primitivi su $\mathbb{Z}$ sono irriducibili in $\mathbb{Z}[x]$.*

DIMOSTRAZIONE. L'irriducibilità su $\mathbb{Z}$ segue da quella su $\mathbb{F}_p$, grazie al teorema 12.56. □

Abbiamo visto nella dimostrazione del teorema 12.56 che se E è un estensione di $\mathbb{F}_p$ che contiene una radice del polinomio di Artin $f_a(x)$, allora per ogni altra radice $\beta \in E$ di $f_a(x)$ si ha $\beta - \alpha \in \mathbb{F}_p$. Questa proprietà caratterizza i polinomi di Artin tra i polinomi monici di grado p diversi dal polinomio $x^p - x$.

Teorema 12.59. *Sia p un primo e sia $f(x)$ un polinomio monico su $\mathbb{F}_p$ di grado p, coprimo con la sua derivata $f'(x)$. Allora per $f(x)$ sono equivalenti le seguenti proprietà:*

(a) per ogni estensione E di $\mathbb{F}_p$ e per ogni coppia di radici $\alpha, \beta \in E$ di $f(x)$ si ha $\beta - \alpha \in \mathbb{F}_p$;
(b) esiste un'estensione E di $\mathbb{F}_p$ contenente il campo di spezzamento di $f(x)$ e tale che per ogni coppia di radici $\alpha, \beta \in E$ di $f(x)$ si ha $\beta - \alpha \in \mathbb{F}_p$;
(c) $f(x) = x^p - x$ oppure $f(x)$ è un polinomio di Artin.

DIMOSTRAZIONE. Come abbiamo notato sopra, l'implicazione (c) $\rightarrow$ (a) è stata già dimostrata nella dimostrazione del teorema 12.56 per i polinomi di Artin. Per il polinomio $f(x) = x^p - x$, (a) è ovvio.

L'implicazione (a) $\rightarrow$ (b) è banale.

Per dimostrare l'implicazione (b) $\longrightarrow$ (c) fissiamo un'estensione E con la proprietà descritta in (b). Notiamo innanzitutto che essa implica due possibilità per le radici di $f(x)$: o sono tutte in $\mathbb{F}_p$, oppure sono tutte in E, ma non appartengono a $\mathbb{F}_p$. Nel primo caso abbiamo $f(x) = x^p - x$, in quanto $f(x)$ ha grado p, è monico ed ha esattamente gli stessi zeri $x^p - x$. Supponiamo ora che esista una radice α di $f(x)$ in E, ma non in $\mathbb{F}_p$. Allora tutte le radici di $f(x)$ sono del tipo $\alpha + k$, con $k \in \mathbb{F}_p$. Per ipotesi queste radici sono diverse. Quindi $\alpha, \alpha+1, \ldots, \alpha+(p-1)$ sono tutte le radici di $f(x)$. Allora, per il teorema di Ruffini,

$$f(x) = (x-\alpha)(x-(\alpha+1))(x-(\alpha+2))\ldots(x-(\alpha+p-1)).$$

Poiché $(x^p - x) = x(x+1)(x+2)\ldots(x+p-1)$ in $\mathbb{F}_p$, sostituendo con α abbiamo $\alpha^p - \alpha = \alpha(\alpha+1)(\alpha+2)\ldots(\alpha+p-1)$. Quindi il termine noto a di $f(x)$ risulta essere uguale a $-(\alpha^p - \alpha)$. Pertanto $\alpha^p - \alpha + a = 0$. Poiché $\alpha \notin \mathbb{F}_p$, si ha $a \neq 0$. Allora α è radice anche del polinomio di Artin $f_a(x)$. Essendo $f_a(x)$ irriducibile per il teorema 12.56, sarà il polinomio minimo di α, e quindi $f(\alpha) = 0$ implica che $f_a(x)$ divide $f(x)$. Essendo questi due polinomi monici dello stesso grado, questo è possibile solo se $f(x) = f_a(x)$. □

È evidente che su di un campo finito vi è solo una quantità numerabile di polinomi, di questi solo un numero finito hanno grado n per un fissato naturale n, e non è difficile calcolare esattamente questo numero. Più difficile è calcolare il numero dei polinomi irriducibili su un campo finito.

Definizione 12.60. Si denota con $N_p(n)$ il numero dei polinomi irriducibili monici di grado n su $\mathbb{F}_p$.

È facile calcolare $N_p(1) = p$ e $N_p(2) = p(p-1)/2$ per ogni primo p, si veda l'esercizio 12.39 per altri esempi. Per il caso generale sarà utile il seguente teorema.

Teorema 12.61. *Sia p un numero primo e sia $g(x)$ un polinomio irriducibile di grado m su $\mathbb{F}_p$. Se $n \in \mathbb{N}$, allora $g(x)$ divide il polinomio $x^{p^n} - x$ se e solo se m divide n.*

DIMOSTRAZIONE. Supponiamo che m divida n. Sia α una radice di $g(x)$ in qualche estensione E di $\mathbb{F}_p$. Poichè $g(x)$ è irriducibile, $g(x)$ sarà il polinomio minimo di α. Essendo il grado di $g(x)$ uguale a m, sappiamo che α appartiene ad una estensione di $\mathbb{F}_p$ di grado m, e quindi ad un campo finito con p^m elementi. Allora α soddisfa l'equazione $\alpha^{p^m} - \alpha = 0$, di conseguenza $\alpha^{p^m} = \alpha$. Elevando questa uguaglianza $\frac{n}{m} - 1$ volte alla p^m otteniamo $\alpha^{p^n} = \alpha$. Questo implica che il polinomio $g(x)$ divide $x^{p^n} - x$.

Supponiamo che $g(x)$ divida il polinomio $f(x) = x^{p^n} - x$. Poiché $g(x)$ è irriducibile, l'anello quoziente $K = \mathbb{F}_p[x]/(g(x))$ è un campo. Essendo K anche finito, abbiamo $|K| = p^m$. Sia $\alpha = x + (g(x)) \in K$; allora $g(\alpha) = 0$. Per ipotesi $g(x)$ divide $f(x)$, quindi anche $f(\alpha) = 0$. Allora α appartiene al campo di spezzamento K_1 del polinomio $f(x)$. Poiché $K = \mathbb{F}_p[\alpha]$, abbiamo anche $K \subseteq K_1$. Quindi $|K_1| = |K|^d$, dove $d = [K_1 : K]$. Da $|K| = p^m$ e $|K_1| = p^n$, concludiamo che $p^n = p^{dm}$ e dunque m divide n. □

Corollario 12.62. *Sia p un numero primo, allora il polinomio $x^{p^p} - x$ è divisibile in $\mathbb{F}_p[x]$ dal seguente polinomio:*

$$(x^p - x) \cdot \prod_{a=1}^{p-1} f_a(x) = x(x-1)\dots(x-p+1) \cdot \prod_{a=1}^{p-1} f_a(x).$$

DIMOSTRAZIONE. Poniamo $f(x) = x^{p^p} - x$. Per il teorema 12.61

$$g(x) = \prod_{a=1}^{p-1} f_a(x) \quad \text{divide} \quad f(x)$$

poiché i polinomi di Artin sono a due a due coprimi. D'altra parte, ogni elemento $a \in \mathbb{F}_p$ soddisfa $a^p = a$, e quindi anche $f(a) = 0$. Questo dimostra che $x^p - x$ divide $f(x)$. Poiché $g(x)$ e $x^p - x$ sono coprimi, anche $(x^p - x)g(x)$ divide $f(x)$. □

Ora diamo un'altra applicazione del teorema 12.61.

Proposizione 12.63. *Sia p un numero primo. Allora $p^n = \sum_{d|n} dN_p(d)$.*

DIMOSTRAZIONE. Applicando il teorema 12.61 avremo

$$x^{p^n} - x = \prod \{g(x) \in \mathbb{F}_p[x] : g(x) \text{ irriducibile monico e } \deg g \text{ divide } n\}.$$

Per la definizione di $N_p(n)$ i fattori di grado d nella parte a sinistra sono $N_p(d)$ quando $d|n$. Quindi calcolando i gradi a destra e sinistra, troviamo $p^n = \sum_{d|n} dN_p(d)$. □

Grazie alla proposizione 12.63 si può calcolare ad esempio $N_p(2^s)$ per ogni primo p e ogni $s \geq 1$, si veda l'esercizio 12.39.

Usando la funzione di Möbius è possibile "invertire" la formula

$$p^n = \sum_{d|n} dN_p(d)$$

esprimendo $N_p(n)$ tramite le potenze di p.

Definizione 12.64. Si dice *funzione di Möbius* la funzione $\mu : \mathbb{N}_+ \to \mathbb{Z}$ definita da

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1 \\ (-1)^r, & \text{se } n = p_1 \cdots p_r \text{ con } p_1, \dots, p_r \text{ numeri primi distinti,} \\ 0, & \text{se } n \text{ è divisibile per il quadrato di qualche numero primo.} \end{cases}$$

Non è difficile dimostrare che $\mu(mn) = \mu(m)\mu(n)$ qualora m ed n siano numeri naturali coprimi tra loro e che se $n > 1$ si ha $\sum_{d|n} \mu(d) = 0$, si veda l'esercizio 12.43.

Per calcolare la formula di $N_p(n)$ per ogni intero n, avremo bisogno della seguente formula dell'inversione di Möbius.

Lemma 12.65. *Sia f una funzione $\mathbb{N}_+ \to \mathbb{Z}$. Allora per la funzione $F : \mathbb{N}_+ \to \mathbb{Z}$ definita da $F(n) = \sum_{d|n} f(d)$ si ha*

$$f(n) = \sum_{d|n} \mu(n/d)F(d).$$

DIMOSTRAZIONE. Si ha

$$\sum_{d|n} \mu(n/d)F(d) = \sum_{e|n} \mu(e)F(n/e) = \sum_{e|n} \left(\mu(e) \sum_{d|(n/e)} f(d) \right) =$$

$$\sum_{d|n} \left(\sum_{e|(n/d)} \mu(e) \right) f(d) = \mu(1)f(n) = f(n).$$

La penultima uguaglianza segue dal fatto che $\sum_{e|(n/d)} \mu(e) = 0$ se $n/d > 1$. Quindi, nella sommatoria resta solo l'addendo relativo a $n/d = 1$, cioè $d = n$. Questo dimostra il lemma. □

Teorema 12.66. *Per la funzione $N_p(n)$ vale la formula $N_p(n) = \frac{1}{n} \sum_{d|n} \mu(n/d)p^d$.*

DIMOSTRAZIONE. Ponendo $f(m) = mN_p(m)$ applichiamo la formula di inversione di Möbius alla formula $p^n = \sum_{d|n} dN_p(d)$. □

Esempio 12.67. Notiamo che la formula dell'inversione è applicabile anche in altre situazioni più generali.

Sia $(G, +)$ un gruppo abeliano e sia $f : \mathbb{N}_+ \to G$ una funzione. Definiamo la funzione $F : \mathbb{N}_+ \to G$ con $F(n) = \sum_{d|n} f(d)$. Allora ripetendo la dimostrazione del teorema 12.65 ricaviamo $f(n) = \sum_{d|n} \mu(n/d)F(d)$. In caso di notazione moltiplicativa del gruppo abeliano $(G, .)$ per una funzione $f : \mathbb{N}_+ \to G$ la funzione $F : \mathbb{N}_+ \to G$ si definisce con $F(n) = \prod_{d|n} f(d)$ e si ha la formula di inversione

$$f(n) = \prod_{d|n} F(d)^{\mu(n/d)}.$$

Applicando l'ultima formula alla (11) del lemma 12.49 ricaviamo

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

12.9 Gli automorfismi di un campo finito

Concludiamo questo paragrafo con lo studio del gruppo degli automorfismi di campo per un qualsiasi campo finito F. Dimostriamo infatti che $\mathrm{Aut}(F)$ è ciclico.

Lemma 12.68. *Sia F un campo finito di caratteristica p, $|F| = p^n$. Allora*

$$\Phi : F \to F \quad \textit{definito da } \alpha \mapsto \alpha^p$$

è un automorfismo di campo di ordine n.

DIMOSTRAZIONE. Innanzitutto Φ è un omomorfismo di campo, in quanto

$$\Phi(a+b) = (a+b)^p = a^p + b^p = \Phi(a) + \Phi(b)$$

in un campo di caratteristica p e

$$\Phi(ab) = (ab)^p = a^p b^p = \Phi(a)\Phi(b)$$

in tutti i campi. Inoltre Φ non è nullo, pertanto Φ è iniettivo e, poiché il campo è finito, è anche suriettivo.

Sia id l'automorfismo identico di F e $k = o(\Phi)$. Per il teorema 12.61, per ogni $a \in F$ si ha $a^{p^n} = a$, da cui $\Phi^n = id$ e quindi $k \leq n$. Poiché $\Phi^k = id$, allora $a^{p^k} = a$ per ogni $a \in F$, cioè F è contenuto nel campo di spezzamento di $x^{p^k} - x$ su $\mathbb{F}_p$. Abbiamo dimostrato nel teorema 12.61 che tale campo ha esattamente cardinalità p^k. Da questo segue $n \leq k$. □

Definizione 12.69. L'*automorfismo di Frobenius* di un campo F di caratteristica p è l'automorfismo Φ definito da $\alpha \mapsto \alpha^p$ per $\alpha \in F$.

Ogni potenza Φ^k di Φ è un automorfismo di F. Vedremo nel teorema 12.73 che questi sono tutti gli automorfismi di F.

Lemma 12.70. *Sia F un campo di caratteristica p, $\mathbb{F}_p$ il suo sottocampo fondamentale e $a \in F$. Allora $\Phi(a) = a$ se e solo se $a \in \mathbb{F}_p$.*

DIMOSTRAZIONE. Sia $a \in F$. Allora $\Phi(a) = a$ significa che $a^p = a$ e cioè che a è radice del polinomio $x^p - x$. Le radici di questo polinomio sono tutti e soli gli elementi di $\mathbb{F}_p$. Pertanto $\Phi(a) = a$ se e solo se $a \in \mathbb{F}_p$. □

Lemma 12.71. *Sia $f(x) \in \mathbb{F}_p[x]$, F un'estensione di $\mathbb{F}_p$ e $\alpha \in F$ una radice di $f(x)$. Se ϕ è un automorfismo di campo di F, allora anche $\phi(\alpha)$ è radice di $f(x)$.*

DIMOSTRAZIONE. Sia $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, con $a_i \in \mathbb{F}_p$ per ogni $i = 1, \ldots, n$. Allora per l'esercizio 12.23, si ha $\phi(a_i) = a_i$ per ogni $i = 1, \ldots, n$ da cui

$$0 = \phi(f(\alpha)) = \phi(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = a_0 + a_1\phi(\alpha) + \ldots + \phi(\alpha)^n = f(\phi(\alpha)).$$

□

Data una radice di un polinomio irriducibile su $\mathbb{F}_p$ si possono ricavare facilmente tutte le restanti radici. Ricordiamo, che per il teorema 12.54 tutte le radici di un polinomio irriducibile su $\mathbb{F}_p$ sono semplici.

Dato un automorfismo φ di un campo K, possiamo estenderlo ad un automorfismo $\overline{\varphi}$ dell'anello $K[x]$, ponendo

$$\overline{\varphi}(k) = \varphi(k) \text{ se } k \in K \text{ e } \overline{\varphi}(x) = x.$$

Lemma 12.72. *Sia p un numero primo e sia $f(x)$ un polinomio irriducibile su $\mathbb{F}_p$ di grado n. Se α è una radice di $f(x)$ in qualche estensione di $\mathbb{F}_p$, allora $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$ sono tutte le radici di $f(x)$.*

DIMOSTRAZIONE. Sia $E = \mathbb{F}_p[\alpha]$, allora, essendo $f(x)$ irriducibile e di grado n, il campo E deve avere p^n elementi; in particolare $\alpha^{p^n} = \alpha$. Sia Φ l'automorfismo di Frobenius di E, per il lemma 12.71 anche $\Phi^s(\alpha)$ è radice di $f(x)$ per ogni $s \in \mathbb{N}$. Sia $S = \{\Phi^s(\alpha) : 0 \leq s \leq n-1\}$: allora S è un insieme invariante per Φ, cioè $\Phi(S) \subseteq S$. Sia

$$g(x) = \prod_{s=0}^{n-1}(x - \Phi^s(\alpha)) = b_0 + b_1 x + \ldots + b_n x^n, \text{ dove } b_i \in E \text{ per ogni } i = 1, \ldots n.$$

Allora, se $\overline{\Phi}$ denota l'automorfismo di $E[x]$ come definito prima di questo lemma, si ha

$$\overline{\Phi}(g(x)) = \overline{\Phi}\left(\prod_{s=0}^{k-1}(x - \Phi^s(\alpha))\right) = g(x),$$

da cui

$$\overline{\Phi}(b_0) + \overline{\Phi}(b_1)x + \ldots + \overline{\Phi}(b_n)x^n = \overline{\Phi}(b_0 + b_1 x + \ldots + b_n x^n) =$$

$$= \overline{\Phi}(g(x)) = g(x) = b_0 + b_1 x + \ldots + b_n x^n.$$

Di conseguenza $\overline{\Phi}(b_i) = \Phi(b_i) = b_i$ per ogni $i = 0, \ldots, n$, da cui $b_i \in \mathbb{F}_p$ per ogni $i = 0, \ldots, n$, per il lemma 12.70. Quindi $g(x) \in \mathbb{F}_p[x]$ e $g(x)$ divide $f(x)$ perché tutte le radici $\Phi^s(\alpha)$ di $g(x)$ sono anche radici di f. Essendo $f(x)$ irriducibile, concludiamo che $g(x) \sim f(x)$. Poiché $f(x)$ non può avere più di n radici, $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$ sono tutte le radici di $f(x)$. □

Teorema 12.73. *Sia F un campo finito e sia Φ il suo automorfismo di Frobenius. Allora ogni automorfismo di F è potenza di Φ, cioè il gruppo $Aut(F)$ è ciclico.*

DIMOSTRAZIONE. Sia p la caratteristica di F. Per il corollario 11.46 sappiamo che il gruppo moltiplicativo del campo F è ciclico. Sia α un generatore di $F \setminus \{0\}$, allora $F = \mathbb{F}_p(\alpha)$. Sia $f(x)$ il polinomio minimo di α su $\mathbb{F}_p$ e sia $n = \deg f$, allora per il lemma 12.72 $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$ sono tutte le radici di $f(x)$. Notiamo adesso che un automorfismo $\xi : F \to F$ è determinato dal valore $\xi(\alpha)$, poiché $F = \mathbb{F}_p[\alpha]$. Per il lemma 12.71, $\xi(\alpha)$ è ancora una radice di $f(x)$, quindi $\xi(\alpha) = \alpha^{p^k}$ con $0 \leq k < n$. Pertanto ξ coincide con Φ^k su α e su $\mathbb{F}_p$, per l'esercizio 12.23. Allora $\xi = \Phi^k$. □

12.10 Alcuni criteri utili per discutere la riducibilità dei polinomi

(a) *Teorema di Ruffini*: Siano A un anello, $a \in A$, $f(x) \in A[x]$. Il polinomio $x - a$ divide $f(x)$ se e solo se $f(a) = 0$.

(b) Siano K un campo, $f(x) \in K[x]$, $\deg(f) = n > 0$. Il numero delle radici di f in K è $\leq n$.

(c) Siano D dominio fattoriale, F il campo dei quozienti di D, $f(x) \in D[x]$, $\deg(f) > 0$. Allora
$f(x)$ irriducibile in $D[x] \Longrightarrow f(x)$ irriducibile in $F[x]$.

(d) *Criterio di Eisenstein*: Sia $f(x) \in \mathbb{Z}[x]$, $f(x) = a_n x^n + \ldots + a_0$ e p un primo tale che:
(1) p divide a_i per ogni $i = 0, \ldots, n-1$;
(2) p non divide a_n;
(3) p^2 non divide a_0.
Allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

(e) *Polinomi di Artin*: Sia $f(x) \in \mathbb{Z}[x]$, $f(x) = a_p x^p + \ldots + a_0$ e p un primo tale che:
(1) p divide a_i per ogni $i = 2, \ldots, p-1$;
(2) p non divide a_0;
(3) $a_p \equiv -a_1 \equiv 1 (mod\, p)$.
Allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$ e $\overline{f}(x) = x^p - x + \overline{a_0}$ è irriducibile in $\mathbb{Z}_p[x]$.

(f) Se K è campo e $f(x) \in K[x]$:
- se $\deg(f) = 1$, allora f è irriducibile;
- se $\deg(f) = 2$ oppure 3, allora f è riducibile se e solo se ha radici in K;
- se $\deg(f) \geq 4$, allora f può essere riducibile e senza radici in K.

(g) Siano $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ e $\frac{r}{s} \in \mathbb{Q}$ uno zero di f, con $(r, s) = 1$. Allora $r | a_0$ ed $s | a_n$.

(h) Gli irriducibili in $\mathbb{R}[x]$ sono:
- i polinomi di grado 1;
- i polinomi di grado 2 con discriminante negativo.

(i) Gli irriducibili in $\mathbb{C}[x]$ sono i polinomi di grado 1.

(j) Siano $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo, $f(x) = a_n x^n + \ldots + a_0$, e p un primo che non divide a_n. Tramite l'omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, si riduce il polinomio modulo p:
$$f(x) = \sum a_k x^k \longmapsto \overline{f}(x) = \sum \overline{a_k} x^k.$$
Allora
- $f(x)$ riducibile in $\mathbb{Z}[x] \Rightarrow \overline{f}(x)$ riducibile in $\mathbb{Z}_p[x]$ e quindi
- $\overline{f}(x)$ irriducibile in $\mathbb{Z}_p[x] \Rightarrow f(x)$ irriducibile in $\mathbb{Z}[x]$.

12.11 Esercizi su campi

Esercizio 12.1 Siano $p \neq q$ numeri primi. Dimostrare che le estensioni semplici $\mathbb{Q}(\sqrt{p})$ e $\mathbb{Q}(\sqrt{q})$ di $\mathbb{Q}$ non sono isomorfe.

Esercizio 12.2 Descrivere il campo di spezzamento del polinomio $f(x) = x^3 - 2$ su $\mathbb{Q}[x]$.

Esercizio 12.3 Provare che ogni campo algebricamente chiuso è infinito.

Esercizio 12.4 Scomporre $x^4 + 4$ in prodotto di polinomi irriducibili su $\mathbb{R}$.

Esercizio 12.5 Sia $u = \sqrt{5 - \sqrt{5}}$.

(a) Provare che u è algebrico su $\mathbb{Q}$.
(b) Determinare il polinomio minimo $f(x)$ di u su $\mathbb{Q}$ e il grado di u su $\mathbb{Q}$.
(c) Scrivere $\frac{1}{u^2}$ come combinazione lineare di u e delle sue potenze.
(d) Dire se $Q(u)$ è campo di spezzamento per $f(x)$ su $\mathbb{Q}$.

Esercizio 12.6 Sia $u = \sqrt[3]{2}i - 1$.

(a) Provare che i e $\sqrt[3]{2} \in \mathbb{Q}(u)$.
(b) Trovare il grado $[\mathbb{Q}(u) : \mathbb{Q}]$.
(c) Dedurre che $\mathbb{Q}(u) = \mathbb{Q}(i, \sqrt[3]{2})$.
(d) Trovare il polinomio minimo di u su $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt[3]{2})$.

Esercizio 12.7 Sia $u = \sqrt[3]{2} + \sqrt[3]{4}$.

(a) Provare che $\mathbb{Q}(u) = \mathbb{Q}(\sqrt[3]{2})$.
(b) Dedurne il grado di u su $\mathbb{Q}$.
(c) Calcolare il polinomio minimo di u su $\mathbb{Q}$.

Esercizio 12.8 Sia $u = \sqrt{2 + \sqrt{6}}$.

(a) Calcolare il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
(b) Dire se $\mathbb{Q}(u)$ è campo di spezzamento per $f(x)$ su $\mathbb{Q}$.
(c) Determinare il campo di spezzamento per $f(x)$ su $\mathbb{Q}$.

Esercizio 12.9 Sia $u = \sqrt{5} - \sqrt{11}$.

(a) Provare che u è algebrico su $\mathbb{Q}$ e determinare il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
(b) Verificare che $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{5}, \sqrt{11})$.
(c) Dire se $\mathbb{Q}(u)$ è campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

Esercizio 12.10 Provare che il polinomio $x^5 - 5x + 1$ è irriducibile su $\mathbb{Q}$.

Esercizio 12.11 Si scrivano 2 polinomi irriducibili, la dimostrazione dell'irriducibilità dei quali, sia una sfida per i colleghi che si sentono più bravi.

Esercizio 12.12 Sia $u = \sqrt{3 + 3\sqrt{2}}$.

(a) Determinare il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
(b) Dire se $\mathbb{Q}(u)$ è campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

Esercizio 12.13 Sia $u = \frac{\sqrt[4]{2}}{1+\sqrt{2}}$.

(a) Calcolare il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
(b) Provare che $\mathbb{Q}(u) = \mathbb{Q}(\sqrt[4]{2})$.
(c) Dire se $\mathbb{Q}(u)$ è campo di spezzamento per $f(x)$ su $\mathbb{Q}$.

Esercizio 12.14 Siano p un primo, $K = \mathbb{F}_p$ e $f(x) = x^p - x - 1 \in K[x]$.

(a) Provare che $f(x)$ non ha radici in K.
(b) Trovare il campo di spezzamento di $f(x)$ su K.
(c) Provare che $f(x)$ è irriducibile su K.

Esercizio 12.15 Si dimostri che i polinomi

$$f(x) = 6x^5 + 10x^4 - 20x^3 + 14x - 2, \quad g(x) = 6x^7 - 7x^6 + 21x^4 - 98x^3 + 8x - 9,$$

$$h(x) = x^{11} - 121x^9 + 22x^7 + 132x^5 - 154x^3 + 10x - 10$$

sono irriducibili in $\mathbb{Q}[x]$.

Esercizio 12.16 Si dimostri che il polinomio $f(x) = 6x^5 - 10x^4 + 10x^3 + 4x - 8$ è polinomio di Artin su $\mathbb{Z}$ e si discuta la riducibilità di $f(x)$ in $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$.

Esercizio 12.17 Siano

$$K = \mathbb{F}_3[x]/(x^2 + 1) \quad \text{e} \quad F = \mathbb{F}_3[x]/(x^2 + x - 1).$$

(a) Dimostrare che K ed F sono campi.
(b) Si dica se sono isomorfi e, se lo sono, costruire esplicitamente un isomorfismo $\varphi : K \to F$.
(c) È possibile costruire un secondo isomorfismo $\psi : K \to F$?

Esercizio 12.18 Determinare gli elementi a di $\mathbb{Z}_5$ per i quali il polinomio

$$f_a(x) = x^2 + x + a$$

è irriducibile in $\mathbb{Z}_5[x]$ e quelli per i quali ha radici multiple.

Esercizio 12.19 Si dimostri che il polinomio

$$f(x) = 12x^{11} - 33x^8 + 22x^6 + 132x^4 + 154x^2 + 10x - 5$$

è irriducibile in $\mathbb{Q}[x]$.

Esercizio 12.20 Si consideri il polinomio $f(x) = x^4 + 1$.

(a) Si dimostri che $f(x)$ è irriducibile in $\mathbb{Q}[x]$.
(b) Sia $K = \mathbb{Q}[x]/(f(x))$, dove $(f(x))$ indica l'ideale principale di $\mathbb{Q}[x]$ generato da $f(x)$. Si dimostri che K è un campo.
(c) Si calcoli il grado $[K : \mathbb{Q}]$.
(d) Si considerino i polinomi $x^2 + 1$ e $x^2 - 2$ come polinomi su K. Quale di questi polinomi è irriducibile e perché?

Esercizio 12.21 Si consideri il polinomio

$$f(x) = 3x^7 + 4x^6 - 9x^5 + 12x^4 - 5x^3 + 6x^2 + 3x + 5$$

e sia I l'ideale di $\mathbb{Z}[x]$ generato da $f(x)$ e 2, $I = (f(x), 2)$. Si dimostri che:

(a) I non è principale;
(b) $f(x)$ è irriducibile in $\mathbb{Q}[x]$;
(c) l'ideale I dell'anello $\mathbb{Z}[x]$ è massimale;
(d) $f(x)$ è riducibile in $\mathbb{Z}_3[x]$.
(e) Sia $K = \mathbb{Q}(\alpha)$ un'estensione tramite una radice α di $f(x)$; calcolare il grado $[K : \mathbb{Q}]$ e dimostrare che $\mathbb{Q}(\alpha^3) = K$.

Esercizio 12.22 Sia E un'estensione del campo K e siano $\alpha_1, \dots, \alpha_n \in E$ elementi algebrici su K. Dimostrare che $K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$.

Esercizio 12.23 Siano F un campo e K il suo sottocampo fondamentale. Sia

$$f : F \to F$$

un automorfismo di campo, si dimostri che $f(k) = k$ per ogni $k \in K$.

Esercizio 12.24 Scomporre $x^4 + 1$ in prodotto di polinomi irriducibili su $\mathbb{R}$.

Esercizio 12.25 Si dimostri che il numero delle radici n-esime primitive dell'unità è pari al numero $\varphi(n)$ degli interi positivi minori di n e con esso coprimi.

Esercizio 12.26 Decomporre il polinomio $x^{11} - x$ nel prodotto di fattori irriducibili in ciascuno degli anelli $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ e $\mathbb{Z}_{11}[x]$.

Esercizio 12.27 Si trovino tutte le coppie $a, b \in \mathbb{Z}_2$ tali che il polinomio

$$g_{a,b}(x) = x^7 + x^3 + ax^2 + bx + 1$$

sia irriducibile in $\mathbb{Z}_2[x]$.

Esercizio 12.28 Sia $\alpha = \sqrt{2} + \sqrt[3]{5}$. Trovare i polinomi minimi di α in $\mathbb{Q}[x]$ e in $\mathbb{Q}(\sqrt{2})[x]$.

Esercizio 12.29 Sia $k \neq n$ un divisore di n. Dimostrare che il polinomio ciclotomico $\Phi_n(x)$ divide il polinomio $\frac{x^n-1}{x^k-1}$.

Esercizio 12.30 Sia F un campo finito e siano $a_1, \dots, a_{n-1}$ tutti gli elementi non nulli di F. Dimostrare che $a_1 \dots a_{n-1} = -1$.

Esercizio 12.31 Sia F un campo finito con 9 elementi: determinare la caratteristica di F. Sia a un elemento di F diverso da 0 e ± 1. Dimostrare che $a^6 + a^4 + a^2 + 1 = 0$.

Esercizio 12.32 Costruire un campo con 625 elementi.

Esercizio 12.33 Trovare un isomorfismo fra i campi

$$Z_{11}[x]/(x^2 + 1) \quad \text{e} \quad Z_{11}[x]/(x^2 + x + 4).$$

Esercizio 12.34 Dimostrare che in $\mathbb{Z}_p$, p primo ci sono al più n soluzioni di $x^n = 1$, per ogni $n \in \mathbb{N}$. È vera la stessa affermazione per $\mathbb{Z}_m$ nel caso in cui m non sia primo?

Esercizio 12.35 Calcolare il prodotto di tutti i polinomi monici irriducibili su $\mathbb{Z}_3$ di grado ≤ 2.

Esercizio 12.36 Quali dei numeri 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 e 20 possono essere cardinalità di un campo finito? Giustificare la risposta.

Esercizio 12.37 Dimostrare che $\mathbb{Q}[x]/(x^4 - 5)$ è un campo e trovare l'inverso di $x^2 + 1$.

Esercizio 12.38 Sia p un numero primo. Dimostrare che il polinomio $x^{p^p} - x$ è divisibile da ogni polinomio di Artin su $\mathbb{F}_p$.

Esercizio 12.39 Calcolare:

(a) $N_p(2^s)$ per ogni primo p e per $s \geq 1$.
(b) $N_2(3)$, $N_2(4)$ e $N_2(5)$, trovando esplicitamente i polinomi irriducibili;
(c) $N_3(2)$, $N_3(3)$, $N_3(4)$.

Esercizio 12.40 Dimostrare che $f(x) = x^3 - 3x - 1$ è irriducibile in $\mathbb{Q}[x]$. Se u è la radice reale di f, trovare l'inverso di $u^2 + 1$ in $\mathbb{Q}[u]$.

Esercizio 12.41 Calcolare esplicitamente i polinomi ciclotomici $\Phi_{12}(x)$, $\Phi_{20}(x)$, $\Phi_{40}(x)$ e $\Phi_{60}(x)$.

Esercizio 12.42 Calcolare il numero dei polinomi di grado n su un qualunque campo finito F.

Esercizio 12.43 Sia μ la funzione di Möbius definita su $\mathbb{N}$. Dimostrare che

$$\mu(mn) = \mu(m)\mu(n)$$

se m ed n sono numeri naturali coprimi tra loro e che $\sum_{d|n} \mu(d) = 0$ se $n > 1$.

Esercizio 12.44 Dimostrare che per la funzione di Eulero $\varphi(n)$ vale la formula

$$\varphi(n) = \sum_{d|n} \mu(n/d)d.$$

Esercizio 12.45 Si provi che il numero $\pi^4 - 3\pi^2 + \pi - 1$ è trascendente sul campo $\mathbb{Q}$.

Esercizio 12.46 Determinare per quali valori del numero intero k il polinomio $f(x) = x^4 + kx^2 + 1$ è irriducibile su $\mathbb{Z}$.

Esercizio 12.47 Sia K un campo di caratteristica zero e sia $f(x)$ un polinomio di grado > 0 su K. Per $k \in \mathbb{N}_+$ un elemento $\alpha \in K$ è una radice di molteplicità k di $f(x)$ se e solo se α e radice di $f(x), f'(x), \ldots, f^{(k-1)}(x)$, ma non è radice di $f^{(k)}(x)$.

Esercizio 12.48 Sia K un campo e sia $f(x)$ un polinomio di grado > 0 su K. Dimostrare che $f'(x) = 0$ se e solo se char $K = p$ per qualche primo p e $f(x)$ ha la forma $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \ldots + a_{kp} x^{kp}$ per qualche $k \in \mathbb{N}_+$ e $a_{ip} \in K$ per $i = 0, 1, \ldots, k$. Inoltre, se K è anche finito, allora $f'(x) = 0$ se e solo se $f(x) = g(x)^p$ per qualche $g(x) \in K[x]$.

Esercizio 12.49 Dimostrare che l'insieme degli elementi algebrici di $\mathbb{R}$ su $\mathbb{Q}$ è numerabile.

Esercizio 12.50 Sia $n > 2$ un numero naturale e sia K il campo di spezzamento del polinomio $\Phi_n(x)$ su $\mathbb{Q}$. Descrivere il gruppo di automorfismi di K.

Esercizio 12.51 Sia G un gruppo ciclico di ordine n. Dimostrare che l'anello gruppale $\mathbb{R}[G]$ definito nell'esercizio 9.20 è isomorfo a $\mathbb{R} \times \mathbb{C}^k$ se $n = 2k + 1$ e a $\mathbb{R} \times \mathbb{R} \times \mathbb{C}^{k-1}$ se $n = 2k$.

Esercizio 12.52 Sia G un gruppo ciclico di ordine n. Dimostrare che l'anello gruppale $\mathbb{Q}[G]$ definito nell'esercizio 9.20 è isomorfo al prodotto $\prod_{d|n} \mathbb{Q}(\xi_d)$, dove $\mathbb{Q}(\xi_d)$ denota il campo di spezzamento del polinomio ciclotomico $\Phi_d(x)$.

Esercizio 12.53 Sia G il gruppo ciclico di ordine 8. Descrivere l'anello gruppale $\mathbb{Q}[G]$.

Esercizio 12.54 Siano G il gruppo ciclico di ordine n e K un campo la cui caratteristica non divide n. Dimostrare che:

(a) l'anello gruppale $K[G] \cong F_1 \times \ldots \times F_s$, ove F_i è estensione finita del campo K di grado d_i e vale $\sum_{i=1}^{s} d_i = n$;
(b) se K è algebricamente chiuso, allora $K[G] \cong K^n$.

Esercizio 12.55 Sia G il gruppo $\mathbb{Z}_2^n$ e sia K un campo di caratteristica diversa da 2 o un anello commutativo unitario dove 2 è invertibile. Dimostrare che l'anello gruppale $K[G]$ è isomorfo a K^{2^n}.

Esercizio 12.56 * Sia G il gruppo $\mathbb{Z}_3 \times \mathbb{Z}_3$. Descrivere l'anello gruppale $\mathbb{R}[G]$.

Svolgimento e suggerimenti per la risoluzione di alcuni esercizi

13.1 Esercizi del capitolo 1

1.4 (a) $\mathcal{P}(S \cap T) \subseteq \mathcal{P}(S)$ e $\mathcal{P}(S \cap T) \subseteq \mathcal{P}(T)$ per l'esercizio 1.2. Per dimostrare l'altra inclusione basta notare che ogni $A \in \mathcal{P}(S) \cap \mathcal{P}(T)$ è contenuto sia in S sia in T, e quindi $A \subseteq S \cap T$ per l'esercizio 1.3.

(b) Sia $A \in \mathcal{P}(S) \cup \mathcal{P}(T)$, allora $A \in \mathcal{P}(S)$ oppure $A \in \mathcal{P}(T)$, cioè $A \subseteq S$ oppure $A \subseteq T$; in ogni caso $A \subseteq S \cup T$. L'inclusione può essere stretta. Infatti, se per esempio $S = \{0, 1, 2\}$, $T = \{0, 3\}$ e $A = \{1, 3\}$, si ha $A \in \mathcal{P}(S \cup T)$, ma $A \notin \mathcal{P}(S) \cup \mathcal{P}(T)$.

(c) Se per esempio $S \subseteq T$, $S \cup T = T$ e $\mathcal{P}(S) \cup \mathcal{P}(T) = \mathcal{P}(T)$. Viceversa supponiamo che $\mathcal{P}(S) \cup \mathcal{P}(T) = \mathcal{P}(S \cup T)$ e che $S \not\subseteq T$. Pertanto esiste $s \in S \setminus T$. Considero $A = \{s\} \cup T \subseteq S \cup T$. Allora $A \notin \mathcal{P}(T)$ e quindi $A \in \mathcal{P}(S)$, cioè $T \subseteq S$.

1.5 (c) Siano a, b, c tre elementi distinti di un insieme X. Si prendano ad esempio gli insiemi $S = \{a, b\}$, $T = \{a, c\}$ e $V = \{b, c\}$. Allora

$$(S \setminus T) \setminus V = \emptyset \neq S \setminus (T \setminus V) = \{b\} \quad \text{e} \quad S \setminus T \neq T \setminus S.$$

1.10 (a) Sia $x \in f^{-1}(B)$, allora, per definizione di immagine inversa, si ha che $f(x) \in B$.

(b) Basta prendere una funzione non suriettiva, per esempio $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ tale che $f(x) = x^2$, e un insieme non contenuto nell'immagine di f, per esempio $B = \{1, 2\}$. Allora

$$f^{-1}(B) = \{1, -1\} \quad \text{e} \quad f(f^{-1}(B)) = \{1\} \neq B.$$

(c) Quando f è suriettiva.

1.11 (a) L'applicazione f non è suriettiva perché $f(X) \subseteq B$, pertanto $f(X) \neq A$, per ogni $X \in \mathcal{P}(A)$. Inoltre f non è iniettiva perché $A \neq B$ e $f(A) = \emptyset = f(B)$.

(b) $f^{-1}(\{B\}) = \mathcal{P}(A \setminus B)$.

1.12 (a) No, perché $A \neq B$ e $f(A) = B = f(B)$.

(b) Si osservi che $f(X) \subseteq B$ e quindi $A \neq f(X)$ per ogni $X \in \mathcal{P}(A)$. Allora $f(\mathcal{P}(A)) \subseteq \mathcal{P}(B)$, ma anzi coincidono poiché se $X \in \mathcal{P}(B)$ si ha $f(X) = X$.

(c)

$$f^{-1}(B) = \{X \in \mathcal{P}(A) : X \supseteq B\}, \qquad f^{-1}(A) = \emptyset,$$

$$f^{-1}(\emptyset) = \{X \in \mathcal{P}(A) : X \cap B = \emptyset\} = \mathcal{P}(A \setminus B).$$

1.13 L'identità $f \circ (f \circ f) = id_A$ implica che f è suriettiva e che $f \circ f$ è iniettiva, quindi nuovamente f è iniettiva. Allora f è biettiva.

1.14 (a) È ovvio.

(b) Se f_* è iniettiva, allora la composizione $f_* \circ j_X$ è iniettiva per il lemma 1.22. Per (a) anche la composizione $j_Y \circ f$ è iniettiva. Dal lemma 1.25 si conclude che f è iniettiva. Una dimostrazione diretta alternativa è la seguente. Supponiamo che f_* sia iniettiva. Siano $a, b \in A$ tali che $f(a) = f(b)$, allora

$$f_*(\{a\}) = f(\{a\}) = \{f(a)\} = \{f(b)\} = f(\{b\}) = f_*(\{b\}).$$

Poiché f_* è iniettiva, si avrà $\{a\} = \{b\}$ e quindi $a = b$.

Sia ora f iniettiva. Supponiamo $f_*(B) = f_*(C)$, con $B, C \in \mathcal{P}(A)$. Supponiamo per assurdo che B non sia contenuto in C. Allora esiste un elemento $b \in B \setminus C$. Poiché

$$f(b) \in f(B) = f_*(B) = f_*(C) = f(C),$$

esiste un elemento $c \in C$ tale che $f(b) = f(c)$, da cui $b = c \in C$, in contraddizione con quanto supposto. Quindi $B \subseteq C$ e analogamente si prova $C \subseteq B$, da cui la tesi $B = C$.

(c) Supponiamo che f_* sia suriettiva. Allora esiste $A \in \mathcal{P}(X)$ con

$$f_*(A) = f(A) = Y,$$

quindi anche $f(X) = Y$ e pertanto f è suriettiva. Se invece f è suriettiva e $C \subseteq Y$, allora $f(f^{-1}(C)) = C$, dunque $C = f_*(f^{-1}(C))$.

1.15 (a) Supponiamo che f^* sia iniettiva. Allora essendo $f^*(Y) = f^*(f(X))$ concludiamo che $Y = f(X)$, cioè f è suriettiva. Viceversa, sia f suriettiva, cioè $Y = f(X)$. Allora $f_* \circ f^* = id_{\mathcal{P}(Y)}$ essendo $f(f^{-1}(B)) = B$ per ogni $B \in \mathcal{P}(Y)$. Quindi, f^* è iniettiva per il lemma 1.25.

(b) Sia f^* suriettiva e supponiamo per assurdo che esistano $x \neq y$ in X con $f(x) = f(y)$. Poiché f^* è suriettiva, esiste $B \in \mathcal{P}(Y)$ tale che $\{x\} = f^*(B)$. Ma $y \in f^*(B)$ e quindi si avrebbe $x = y$. Da questa contraddizione concludiamo che f è iniettiva. Supponiamo ora che f sia iniettiva e $A \in \mathcal{P}(X)$, allora $f^{-1}(f(A)) = A$, cioè $A = f^*(f(A))$. Questo dimostra che f^* è suriettiva.

1.16 L'idea è di definire $f(a_1) = a_2$ e proseguire definendo $f(s_1(a_1)) = s_2(a_2)$ e così via: se $f(n)$ è stata definita per un certo $n \in N_1$, definiamo $f(s_1(n)) = s_2(f(n))$. Sia $E = \{n \in N_1 : f(n)$ è definita$\}$. Allora $a_1 \in E$ e se $n \in E$, allora

anche $s_1(n) \in E$ essendo $f(s_1(n)) = s_2(f(n))$ definito. Pertanto per (P5), si ha $E = N_1$, quindi f è definita su tutto N_1. Resta da provare che f è una biezione.

Sia $A = \{p \in N_2 : \text{esiste } n \in N_1 \text{ con } f(n) = p\}$. Allora $a_2 = f(a_1) \in A$, e se $p \in A$, allora $p = f(n)$, da cui $s_2(p) = s_2(f(n)) = f(s_1(n))$ e quindi $s_2(p) \in A$. Pertanto per (P5), $A = N_2$ e f è suriettiva.

Sia $I = \{m \in N_1 : \text{se } f(m) = f(n) \text{ per qualche } n \in N_1, \text{ allora } m = n\}$. Allora $a_1 \in I$ perché se $f(a_1) = f(n)$ per qualche $n \in N_1$ e supponiamo per assurdo $n \neq a_1$, esiste $\tilde{n} \in N_1$, con $n = s_1(\tilde{n})$ da cui

$$a_2 = f(a_1) = f(n) = f(s_1(\tilde{n})) = s_2(f(\tilde{n}))$$

che contraddice (P3). Sia ora $m \in I$, e supponiamo $f(s_1(m)) = f(n)$, per qualche $n \in N_1$. Poiché $s_1(m) \neq a_1$, per quanto appena provato si ha $n \neq a_1$, pertanto esiste $\tilde{n} \in N$, con $n = s_1(\tilde{n})$ da cui

$$s_2(f(m)) = f(s_1(m)) = f(n) = f(s_1(\tilde{n}) = s_2(f(\tilde{n}))$$

che implica $f(m) = f(\tilde{n})$ perché s_2 è iniettiva e infine $m = \tilde{n}$, in quanto $m \in I$. Allora $s_1(m) = s_1(\tilde{n}) = n$, cioè $s_1(m) \in I$. Concludiamo che $I = N_1$ per (P5), da cui f è iniettiva.

1.17 Ragioniamo per induzione su k. Se $k = 1$, allora l'asserto è vero per $m = n = 0$. Supponiamo $k > 1$ e che l'asserto sia vero per tutti numeri naturali $< k$. Se k è dispari, allora $k = 2m + 1$ e basta prendere $n = 0$. Supponiamo che $k = 2k_1$ sia pari. Allora $k_1 < k$, pertanto $k_1 = 2^m(2n + 1)$ per un opportuna coppia (m, n). Chiaramente $k = 2^{m+1}(2n + 1)$.

Ora supponiamo di avere $k = 2^m(2n + 1)$ e $k_1 = 2^{m_1}(2n_1 + 1)$. Dimostreremo che le due coppie (m, n) e (m_1, n_1) coincidono ragionando per induzione su m. Osserviamo che $m = 0$ se e solo se $m_1 = 0$ non potendo k essere pari e dispari simultaneamente. Se $m = m_1 = 0$ ricaviamo immediatamente anche $n = n_1$. Questo prova che l'asserto è vero per $m = 0$. Se $m > 0$, allora anche $m_1 > 0$ e dall'uguaglianza $2^m(2n+1) = 2^{m_1}(2n_1+1)$ ricaviamo $2^{m-1}(2n+1) = 2^{m_1-1}(2n_1+1)$. Per l'ipotesi induttiva $(m - 1, n) = (m_1 - 1, n_1)$ quindi $(m, n) = (m_1, n_1)$.

1.23 Ragionando per induzione su n supponiamo di avere $(\sum_{k=1}^{n-1} a_k)^2 \leq \sum_{k=1}^{n-1} a_k^3$. Allora, osservando che l'insieme $\{a_1, \ldots, a_{n-1}\} \subseteq \{1, 2, \ldots, a_{n-1}\}$, si ha

$$\sum_{k=1}^{n-1} a_k \leq \sum_{k=1}^{a_{n-1}} k = \frac{(1 + a_{n-1})a_{n-1}}{2} \leq \frac{a_n(a_n - 1)}{2}. \tag{1}$$

Da (1) si ricava

$$2\left(\sum_{k=1}^{n-1} a_k\right) + a_n \leq a_n^2$$

e di conseguenza

$$2a_n\left(\sum_{k=1}^{n-1} a_k\right) + a_n^2 \leq a_n^3.$$

Aggiungendo ad entrambi i membri $(\sum_{k=1}^{n-1} a_k)^2$ si ha

$$\left(\sum_{k=1}^{n} a_k\right)^2 \leq \left(\sum_{k=1}^{n-1} a_k\right)^2 + a_n^3.$$

L'ipotesi induttiva permette di proseguire la disuguaglianza

$$\left(\sum_{k=1}^{n-1} a_k\right)^2 + a_n^3 \leq \sum_{k=1}^{n} a_k^3.$$

1.25 L'errore consiste nell'applicazione scorretta del principio di induzione. Nel passaggio da $n-1$ ad n ad n si sfrutta implicitamente il fatto che $n > 2$ per poter affermare che gli insiemi $\{C_1, \dots, C_{n-1}\}$ e $\{C_2, \dots, C_n\}$ hanno intersezione non vuota.

1.26 Eleviamo tutto alla n, allora dobbiamo dimostrare che la seguente proprietà $A(n)$

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n \leq \left(\frac{a_1 + a_2 + \ldots + a_n}{n}\right)^n$$

vale per ogni n-upla $a_1, \dots, a_n$ in $\mathbb{R}_+$. Si verifica facilmente che $A(1)$ ed $A(2)$ sono vere. Verifichiamo ora che $A(t)$ implica $A(2t)$ per ogni $t \geq 1$. Infatti, siano $a_1, a_2, \dots, a_{2t}$ numeri reali positivi. Essendo $A(t)$ vera si ha

$$a_1 \cdot a_2 \cdot \ldots \cdot a_t \leq \left(\frac{a_1 + a_2 + \ldots + a_t}{t}\right)^t, \tag{2}$$

ma anche

$$a_{t+1} \cdot a_{t+2} \cdot \ldots \cdot a_{2t} \leq \left(\frac{a_{t+1} + a_{t+2} + \ldots + a_{2t}}{t}\right)^t. \tag{3}$$

Moltiplichiamo tra loro le disuguaglianze (2) e (3) e otteniamo

$$a_1 \cdot a_2 \cdot \ldots \cdot a_t \cdot a_{t+1} \cdot a_{t+2} \cdot \ldots \cdot a_{2t} \leq$$

$$\leq \left(\frac{a_1 + a_2 + \ldots + a_t}{t}\right)^t \cdot \left(\frac{a_{t+1} + a_{t+2} + \ldots + a_{2t}}{t}\right)^t. \tag{4}$$

Considerando ora i due fattori del secondo membro della disuguaglianza così ottenuta e utilizzando $A(2)$ già dimostrata, si ha, elevando alla t,

$$\left(\frac{a_1 + a_2 + \ldots + a_t}{t}\right)^t \cdot \left(\frac{a_{t+1} + a_{t+2} + \ldots + a_{2t}}{t}\right)^t \leq$$

$$\leq \left(\frac{a_1 + a_2 + \ldots + a_t + a_{t+1} + a_{t+2} + \ldots + a_{2t}}{2t}\right)^{2t}.$$

Mettendo assieme l'ultima disuguaglianza e la disuguaglianza (4) si ottiene la tesi.

Supponiamo $m > 2$ e $V(k)$ vera per tutti i k con $1 \leq k < m$. Consideriamo due casi. Se $m = 2t$, allora $2 \leq t < m$ e quindi possiamo supporre che $A(t)$ sia vera. Per il fatto appena dimostrato questo implica anche $A(2t)$ è vera. Si ottiene, dunque, la tesi nel caso m pari.

Supponiamo ora $m = 2t - 1$, allora $2 < m$ e quindi $2 \leq t = (m+1)/2 < m$. Possiamo supporre che $A(t)$ sia vera. Per il fatto appena dimostrato, questo implica che anche $A(2t)$ è vera. La applicheremo ai numeri $a_1, a_2, \dots, a_{2t-1}, s$, dove

$$s = \frac{a_1 + a_2 + \ldots + a_{2t-1}}{2t-1}$$

è la media aritmetica. La disuguaglianza per il caso di $2t$ fattori porge:

$$a_1 \cdot a_2 \cdot \ldots \cdot a_{2t-1} \cdot s \leq \left(\frac{(a_1 + a_2 + \ldots + a_{2t-1}) + s}{2t} \right)^{2t}.$$

Ora $a_1 + a_2 + \ldots + a_{2t-1} = s(2t-1)$ e quindi sostituisco nel secondo membro della precedente disuguaglianza e divido tutto per s, ottenendo

$$\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_{2t-1} \cdot s}{s} \leq \left(\frac{s(2t-1) + s}{2t} \right)^{2t} \frac{1}{s} = \frac{s^{2t}}{s}.$$

Eliminando s e risostituendo l'espressione per s otteniamo

$$a_1 \cdot a_2 \cdot \ldots \cdot a_{2t-1} \leq s^{2t-1} = \left(\frac{a_1 + a_2 + \ldots + a_{2t-1}}{2t-1} \right)^{2t-1}$$

1.27 Si usi l'esercizio 1.26.

1.28 Per il lemma 1.37, la prima affermazione è dimostrata.

Proponiamo una dimostrazione della seconda basata sull'uguaglianza

$$\left| \bigcup_{k=1}^{n} A_k \right| = \sum_{k=1}^{n} |A_k|, \tag{5}$$

dove $X = \bigcup_{k=1}^{n} A_k$ è una partizione in insiemi finiti A_k. L'uguaglianza (5) segue dal fatto che se

$$Y = \bigcup_{k=1}^{n} B_k$$

è un altra partizione tale che esistono biezioni $f_k : B_k \to A_k$ per $k = 1, 2, \dots, n$, allora esiste anche un biezione $f : Y \to X$; questa proprietà è una caso particolare dell'esercizio 1.58. Ora, per ricavare (5) nel caso $n = 2$ basta notare che se

$$|A_1| = m_1 \quad \text{e} \quad |A_2| = m_2$$

allora esistono biezioni

$$f_k : \{1, 2, \ldots, m_k\} \to A_k, \quad k = 1, 2.$$

Sia

$$g : \{m_1 + 1, m_1 + 2, \ldots, m_1 + m_2\} \to A_2$$

la biezione definita da $g(m_1 + s) = f_2(s)$. Osserviamo che

$$\{1, 2, \ldots, m_1 + m_2\} = \{1, 2, \ldots, m_k\} \cup \{m_1 + 1, m_1 + 2, \ldots, m_1 + m_2\}.$$

Allora f_1 e g danno luogo ad una biezione

$$f : \{1, 2, \ldots, m_1 + m_2\} \to A_1 \cup A_2.$$

Questo dimostra (5) nel caso $n = 2$. Ora il caso generale segue banalmente per induzione su n.

Tornando all'asserto dell'esercizio, notiamo che ci sono tre partizioni

$$A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B),$$

$$A = (A \setminus B) \cup (A \cap B) \quad \text{e} \quad B = (B \setminus A) \cup (A \cap B).$$

Applicando (5) troviamo

$$|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B|,$$

$$|B| = |B \setminus A| + |A \cap B| \quad \text{e} \quad |A| = |A \setminus B| + |A \cap B|.$$

Ora si conclude facilmente.

1.29 Usare la formula (5) ragionando analogamente alla seconda dimostrazione nello svolgimento dell'esercizio 1.28.

1.30 Scegliamo $x \in X \setminus f(X)$ e definiamo un'applicazione iniettiva $h : \mathbb{N} \to X$ con $h(0) = x$. Cominciamo ponendo $h(0) = x$. Supponendo di aver definito $h(n)$ per qualche $n \in \mathbb{N}$, poniamo $h(n + 1) = f(h(n))$. Allora l'insieme A di tutti gli $n \in \mathbb{N}$ per i quali $h(n)$ è definito contiene 0 e se $n \in A$, allora anche $n + 1 \in A$. Quindi $A = \mathbb{N}$ per il principio di induzione. In questo modo $h : \mathbb{N} \to X$ è stata definita. Supponiamo per assurdo che h non sia iniettiva. Allora esistono $n < m$ in $\mathbb{N}$ con $h(n) = h(m)$. Consideriamo l'insieme

$$B = \{n \in \mathbb{N} : h(n) = h(m) \text{ per qualche } m > n\}$$

e supponiamo per assurdo che B non sia vuoto. Pertanto per il principio del minimo di $\mathbb{N}$, esiste un elemento minimo n di B. Se n fosse diverso da 0, allora

$$f(h(n-1)) = h(n) = h(m) = f(h(m-1)).$$

Per l'iniettività di f concludiamo che $h(n - 1) = h(m - 1)$ e quindi $n - 1 \in B$ contrariamente alla scelta di n come elemento minimo di B. Pertanto $n = 0$ e quindi $h(0) = h(m)$ per qualche $m > 0$. Ora

$$x = h(0) = h(m) = f(h(m-1))$$

contraddice la scelta di x con $x \in X \setminus f(X)$. L'assurdo dimostra che h è iniettiva.

1.37 Per ipotesi esiste una biezione $f : I \to A$, dove $I = \{1, 2, \dots, n\}$ o $I = \mathbb{N}$. In entrambi i casi I ammette un buon ordine $\leq$, che si trasporta su A ponendo per definizione $f(a) \leq f(b)$ qualora $a \leq b$ in I.

1.39 Consideriamo l'insieme Y di tutti i divisori di 15 ordinato per divisibilità:

$$Y = \{1, 3, 5, 15\} \text{ e } a \preceq b \text{ se e solo se } a|b.$$

Allora $(Y, \preceq) = (Y, |)$ è un reticolo e non è totalmente ordinato perché 3 non divide 5 e 5 non divide 3. Il sottoinsieme parzialmente ordinato $X = \{3, 5\}$ non è un reticolo perché $3 \vee 5 = 15$ non esiste in X.

1.41 Grazie al teorema 1.46, è sufficiente calcolare il numero delle partizioni su un insieme di 2, 3, 4 o 5 elementi. Si lasciano al lettore i primi 3 casi: le risposte sono 2, 5 e 15 rispettivamente.

Sia ora $X = \{a, b, c, d, e\}$. Contiamo le partizioni di X:
- 1 del tipo $\{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}\}$;
- 1 del tipo $\{a, b, c, d, e\}$,
- 5 del tipo $\{\{a\}, \{b, c, d, e\}\}$,
- 10 del tipo $\{\{a, b\}, \{c, d, e\}\}$,
- 10 del tipo $\{\{a\}, \{b\}, \{c, d, e\}\}$,
- 15 del tipo $\{\{a, b\}, \{c, d\}, \{e\}\}$,
- 10 del tipo $\{\{a, b\}, \{c\}, \{d\}, \{e\}\}$;

per un totale di 52 partizioni e relazioni di equivalenza.

1.42 Ragionare per induzione.

1.43 (a) Sia a un minimo di X. Se b è un altro minimo, allora $a \leq b$ e $b \leq a$, e pertanto per la proprietà antisimmetrica $a = b$.

(b) segue da (a) e dalla definizione di estremo superiore (inferiore).

1.44 Se a è massimo, $a \geq x$ per ogni $x \in A$, pertanto se si ha $a \leq b$ si conclude che $a = b$, cioè massimale.

Viceversa supponiamo a massimale. Sia b un elemento di A, poiché l'ordine è totale $a \leq b$ oppure $b \leq a$. Se $a \leq b$, dal fatto che a è massimale si deduce che $a = b$, pertanto in ogni caso si ha $b \leq a$.

1.45 Riflessiva: $n|n$ perché $n = 1n$,

antisimmetrica: $n|m$ e $m|n$ implicano $m = rn = r(qm)$, cioè $rq = 1$ e $r, q \in \mathbb{N}$ implicano $r = q = 1$, cioè $m = n$,

transitiva: $n|m$ e $m|l$ implicano $l = qm = q(rn) = (rq)n$, cioè $n|l$.

Il minimo deve essere un elemento x di $\mathbb{N}$ tale che $x|n$ per ogni $n \in \mathbb{N}$, cioè $x = 1$. Il massimo y invece deve essere tale che $n|y$ per ogni $n \in \mathbb{N}$, cioè $y = 0$.

1.46 Le catene di lunghezza 4 sono tre: $\{1, 2, 4, 20\}$, $\{1, 2, 10, 20\}$ e $\{1, 5, 10, 20\}$. Inoltre notiamo che tra tutte le coppie non ordinate di due divisori distinti di 20, solo $\{2, 5\}$, $\{5, 4\}$ e $\{4, 10\}$ non formano una catena.

1.47 Se a è massimale, allora se $a \leq x$, si ha $a = x$ per ogni $x \in X$. Sia dunque $z \in X$ e sia $b = a \vee z$. Allora $b \geq a$, quindi $a = b$, cioè $a \geq z$. Concludiamo che a è massimo.

1.48 Tra i divisori propri di 30 gli elementi minimali sono 2, 3, 5 e gli elementi massimali sono 6, 10 e 15.

Tra i divisori propri di 56 gli elementi minimali sono 2 e 7 e gli elementi massimali sono 8 e 28.

Tra i divisori propri di 120 gli elementi minimali sono 2, 3, 5 e gli elementi massimali sono 60, 40 e 24.

1.50 Supponiamo $n \leq m$, allora una catena di lunghezza $m + n - 1$ è

$$\{(1,1),(2,1),(3,1),\ldots,(n,1),(n,2),(n,3),\ldots,(n,m)\}.$$

Ora dimostrare che ogni catena in X ha lunghezza $\leq m + n - 1$.

1.51 Applicare l'esercizio 1.50.

1.52 Dimostriamo che dati due elementi f, g di L^X, questi ammettono massimo e minimo. Definiamo la funzione $h(x) = f(x) \vee g(x)$: è ben definita perché L è un reticolo e $f(x), g(x)$ sono due elementi del reticolo. Allora $h = f \vee g$. Analogamente per l'estremo inferiore.

1.53 La dimostrazione che $\mathcal{R}$ sia una relazione d'ordine deriva dal fatto che $\leq$ è una relazione d'ordine in S. Vediamo per esempio la dimostrazione della proprietà antisimmetrica:

$f\mathcal{R}g$ e $g\mathcal{R}f$ implicano che $f(x) \leq g(x)$ e $g(x) \leq f(x)$ per ogni $x \in S$. Per la proprietà antisimmetrica di $\leq$, si ha $f(x) = g(x)$ per ogni $x \in S$, cioè $f = g$.

Supponiamo che $\mathcal{R}$ sia di ordine totale e supponiamo che esistano due elementi distinti x ed y in S. Consideriamo la funzione $f : S \to S$ tale che

$$f(x) = y, \quad f(y) = x \quad \text{e} \quad f(z) = z \text{ per ogni altro } z \in S, z \neq x, z \neq y.$$

Allora f ed id_S sono due elementi di S^S, pertanto devono essere confrontabili rispetto alla relazione $\mathcal{R}$. Allora si avrà o $f\mathcal{R}id_S$ oppure $id_S\mathcal{R}f$. Nel primo caso si ha $f(x) = y \leq id_S(x) = x$ e $f(y) = x \leq id_S(y) = y$, da cui si ricava $x = y$. Si conclude allo stesso modo nel secondo caso.

Se S contiene solo un elemento, allora anche S^S contiene solo un elemento e l'ordine è totale.

1.54 Per ogni funzione $f : X \to \{0,1\}$ si ha

$$f = \varphi(\{x \in X : f(x) = 1\}),$$

pertanto φ è suriettiva. D'altra parte, se $\chi_A = \chi_B$, allora $A = B$. Infatti, se $a \in A$, allora $\chi_B(a) = \chi_A(a) = 1$, perciò $a \in B$ e dunque $A \subseteq B$. Analogamente si vede che $B \subseteq A$ e quindi $A = B$. Questo dimostra che φ è anche iniettiva.

1.57 (a) Considerare la corrispondenza $((a_1, a_2, \ldots a_{n-1}), a_n) \mapsto (a_1, a_2, \ldots, a_n)$.
(b) Daremo una dimostrazione per induzione su n. Sia $A(n)$ l'affermazione che la

formula è vera per tutte le n-uple di insiemi finiti $A_1, A_2, \ldots, A_n$. Ovviamente $A(1)$ è vera. Supponiamo ora che siano vere tutte le $A(k)$ con $k < n$. Poniamo $B = A_1 \times A_2 \times \ldots \times A_{n-1}$. Allora $|A_1 \times A_2 \times \ldots \times A_{n-1} \times A_n| = |B \times A_n|$. Per l'ipotesi induttiva

$$|B \times A_n| = |B| \cdot |A_n| \quad \text{e} \quad |B| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_{n-1}|.$$

Ora la tesi segue immediatamente.

1.60 Da $|A| \leq |B|$ concludiamo che esiste un'iniezione $f : A \to B$. Per definire un'applicazione suriettiva $g : B \to A$ scegliamo un elemento arbitrario $a_0 \in A$ e poniamo $g(b) = a$ se risulta $b = f(a)$ per qualche $a \in A$, che è necessariamente unico. Se $b \in B \setminus f(A)$ poniamo $g(b) = a_0$. Se esiste un'applicazione suriettiva $B \to A$, allora il teorema 1.63 implica che esiste un'applicazione iniettiva $A \to B$, e quindi vale $|A| \leq |B|$.

1.61 La funzione lineare $l_1 : [0,1] \to [-1,1]$ definita da $l_1(x) = 2x - 1$ è una biezione. Verificare che l'applicazione $h : [-1,1] \to (-1,1)$ definita da

$$h(x) = \begin{cases} \frac{1}{n+1}, & \text{se } x = \frac{1}{n} \text{ con } n \in \mathbb{Z} \text{ e } n > 0 \\ \frac{1}{n-1}, & \text{se } x = \frac{1}{n} \text{ con } n \in \mathbb{Z} \text{ e } n < 0 \\ x, & \text{se } nx \neq 1 \text{ per tutti gli } n \in \mathbb{Z} \end{cases}$$

è una biezione. Infine la funzione $f : (-1,1) \to \mathbb{R}$ definita da $f(x) = \arctan \frac{\pi x}{2}$, è una biezione. Basta prendere la composizione $f \circ h \circ l_1 : [0,1] \to \mathbb{R}$.

1.62 Notiamo che $|X| \leq |\mathcal{P}(X)|$ in quanto esiste l'applicazione $j_X : X \to \mathcal{P}(X)$ che manda ogni elemento $x \in X$ nel singoletto $\{x\}$ e tale applicazione è iniettiva. Per dimostrare che non vale $|X| \geq |\mathcal{P}(X)|$ basta applicare il teorema di Cantor 1.18.

1.64 (a) Per vedere che $\mathbb{Z}$ è numerabile definiamo un'applicazione $h : \mathbb{Z} \to \mathbb{N}$ con

$$h(n) = \begin{cases} 2n, & \text{se } n \geq 0 \\ -1 - 2n & \text{se } n < 0 \end{cases}$$

Non è difficile verificare che h è biettiva. Questo dimostra che $\mathbb{Z}$ è numerabile e implica anche che $\mathbb{Z} \times \mathbb{Z}$ è numerabile per il lemma 1.74.

Poiché ogni numero razionale r si può scrivere almeno in un modo come

$$r = \frac{a}{b}, \text{ con } a, b \in \mathbb{Z} \text{ e } b \neq 0,$$

esiste una suriezione $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$. Poiché $\mathbb{Z} \times \mathbb{Z}$ è numerabile, allora anche $\mathbb{Q}$ risulta numerabile.

(b) Per vedere che $\bigcup_{n=1}^{\infty} A_n$ è numerabile basta trovare una suriezione

$$f : \mathbb{N} \times \mathbb{N} \to \bigcup_{n=1}^{\infty} A_n.$$

Sia $f_n : \mathbb{N} \to A_n$ una suriezione che testimonia la numerabilità di A_n. Definiamo f con $f(n, m) = f_n(m)$ per ogni $n, m \in \mathbb{N}$.

Per la seconda parte si usi induzione su k e il lemma 1.74.

1.65 Per ogni $i \in I$ scegliamo una biezione $h_i : X_i \to Y_i$, che proviene dal fatto che $|X_i| = |Y_i|$. Ora definiamo $h : X \to Y$ ponendo $h(x) = h_i(x)$, se $x \in X_i$. È sufficiente verificare che h è una biezione.

1.66 Consideriamo la famiglia $\mathfrak{A}$ di tutte le famiglie $\mathcal{A} = \{X_i : i \in I\}$ di sottoinsiemi numerabili a due a due disgiunti X_i di X. Ordiniamo $\mathfrak{A}$ per inclusione. Allora $(\mathfrak{A}, \subseteq)$ è un insieme ordinato induttivo. Infatti, se $\mathfrak{C}$ è una catena in $\mathfrak{A}$, allora $\bigcup \mathfrak{C} \in \mathfrak{A}$, poiché $A, B \in \bigcup \mathfrak{C}$ implica che A e B appartengono allo stesso membro della catena $\mathfrak{C}$ e quindi sono disgiunti. Inoltre $\bigcup \mathfrak{C}$ contiene ogni membro di $\mathfrak{C}$ e quindi è un maggiorante di $\mathfrak{C}$ in $(\mathfrak{A}, \subseteq)$. Quindi possiamo applicare il lemma di Zorn ad $(\mathfrak{A}, \subseteq)$ e affermare che esiste una famiglia massimale $\mathcal{M} = \{X_i : i \in I\} \in \mathfrak{A}$. Sia $Y = \bigcup\{X_i : X_i \in \mathcal{M}\}$. Allora $X \setminus Y$ è finito. Infatti se fosse infinito, esisterebbe un suo sottoinsieme numerabile $Z \subseteq X \setminus Y$ e la famiglia $\{Z\} \cup \mathcal{M} \in \mathfrak{A}$ e contiene strettamente $\mathcal{M}$, assurdo. Aggiungendo l'insieme finito $X \setminus Y$ a qualche membro X_{i_0} di $\mathcal{M}$ troviamo una famiglia $\mathcal{M}' = \{X_{i_0} \cup (X \setminus Y)\} \cup \{X_i : i \in I, i \neq i_0\} \in \mathfrak{A}$. Inoltre $\mathcal{M}'$ è una partizione di X e quindi $\mathcal{M}'$ è la partizione desiderata.

1.67 Sia $\{X_i : i \in I\}$ una partizione di X in insiemi numerabili, che esiste per l'esercizio 1.66. Allora $|X_i \times \{0,1\}| = |X_i|$ per ogni $i \in I$ per il teorema 1.79. Poiché $\{X_i \times \{0,1\} : i \in I\}$ è una partizione di $X \times \{0,1\}$, basta applicare l'esercizio 1.33.

1.68 Per l'esercizio 1.67, esiste una biezione $f : X \to X \times \{0,1\}$. Ora se poniamo $X_i = f^{-1}(X \times \{i-1\})$ per $i = 1, 2$ abbiamo la partizione desiderata.

13.2 Esercizi del capitolo 2

2.1 Supponiamo per assurdo che questa intersezione non sia vuota, allora esiste $x \in \mathbb{R}$ che appartiene a $\bigcap_{n=1}^{\infty}]n, +\infty[$. Sia n_0 la parte intera di x, $n_0 = \lfloor x \rfloor$. Allora x non appartiene all'insieme $]n_0 + 1, \infty[$ e pertanto non può appartenere a quell'intersezione.

2.2 Per dimostrare l'uguaglianza tra due insiemi, si dimostra l'inclusione del primo nel secondo e del secondo nel primo, nota come *doppia inclusione*. Nel nostro caso $0 \in]-\frac{1}{n}, +\frac{1}{n}[$ per ogni $n \in \mathbb{N}$, $n \geq 1$. Questo dimostra l'inclusione "$\supseteq$". Dimostriamo quindi che

$$\bigcap_{n=1}^{\infty} \left] -\frac{1}{n}, +\frac{1}{n} \right[\subseteq \{0\}.$$

Sia $x \in \bigcap_{n=1}^{\infty}]-\frac{1}{n}, +\frac{1}{n}[$. Se $x \neq 0$, sia $|x^{-1}| = |x|^{-1}$ il modulo del suo inverso. Sia $n_0 = \lfloor |x^{-1}| \rfloor$, allora $n_0 \leq |x^{-1}| < n_0 + 1$, da cui si ricava $|x| > \frac{1}{n_0+1}$ e quindi

$$x \notin \left]-\frac{1}{n_0+1}, +\frac{1}{n_0+1}\right[.$$

Pertanto se $x \neq 0$, x non può appartenere a quella intersezione, da cui si deduce che l'unico elemento contenuto nell'intersezione è 0.

2.3 Per $j = 0, 1, \ldots, n$ poniamo $a_j = j\alpha - \lfloor j\alpha \rfloor$ e per $j = 0, 1, \ldots, n-1$ consideriamo l'intervallo $\Delta_j = \left[\frac{j}{n}, \frac{j+1}{n}\right]$. Allora gli $n+1$ numeri a_j sono a due e due distinti, perché α è irrazionale, e sono disposti in n intervalli Δ_j. Per il principio di Dirichlet, esiste j tale che $a_s, a_t \in \Delta_j$ con $1 \leq s < t \leq n$. Quindi

$$|(s-t)\alpha - k| = |a_s - a_t| < 1/n$$

per qualche $k \in \mathbb{Z}$. Poiché $0 < |s-t| \leq n-1$, questo risponde anche al secondo quesito.

2.5 Traslando per $-z_1$, la retta l in questione diventa una retta che passa per l'origine e per il punto $z_2 - z_1$ ed è pertanto definita dai punti $\{\lambda(z_2 - z_1) : \lambda \in \mathbb{R}\}$. Ora traslando questa retta per z_1 troviamo che la retta l è definita dai punti

$$z_1 + \lambda(z_2 - z_1) = (1-\lambda)z_1 + \lambda z_2$$

per $\lambda \in \mathbb{R}$. I punti del segmento $[z_1, z_2]$ sono ottenuti con $0 \leq \lambda \leq 1$.

2.7 Rappresentiamo il triangolo nel piano di Argand-Gauss. Traslandolo possiamo supporre che uno dei vertici coincida con l'origine 0 e pertanto i vertici del triangolo saranno 0, a e b con $a, b \in \mathbb{C}$. Usando gli esercizi precedenti si vede facilmente che i punti della mediana che passa per 0 sono della forma $\mu\frac{a+b}{2}$, mentre i punti della mediana che passa per b sono della forma

$$\lambda\frac{a}{2} + (1-\lambda)b,$$

dove $\mu, \lambda \in \mathbb{R}$. Il punto m dell'intersezione di queste due mediane corrisponde a valori di μ e λ che soddisfano

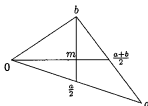
$$\lambda\frac{a}{2} + (1-\lambda)b = \mu\frac{a+b}{2}.$$

Da questo segue

$$\left(\frac{\mu}{2} - \frac{\lambda}{2}\right)a + \left(\frac{\mu}{2} + \lambda - 1\right)b = 0.$$

Poiché i vettori a e b sono linearmente indipendenti, abbiamo

$$\frac{\mu}{2} - \frac{\lambda}{2} = 0 \quad \text{e} \quad \frac{\mu}{2} + \lambda - 1 = 0.$$

Di conseguenza $\mu = \lambda = \frac{2}{3}$. Si noti che il punto di intersezione $m = \frac{a+b}{3}$ divide entrambe le mediane in rapporto $2:1$.

Analogamente si dimostra che la mediana che passa per il punto a passa anche per il punto m.

2.9 Se a, b, c, d sono i quattro vertici di un quadrangolo, i punti medi sono

$$\frac{a+b}{2}, \quad \frac{b+c}{2}, \quad \frac{c+d}{2} \quad \text{e} \quad \frac{d+a}{2}.$$

Ora basta applicare l'esercizio 2.8.

2.11 L'area S del triangolo coincide con il prodotto $\frac{|a|\cdot|b|\cdot\sin\varphi}{2}$, dove φ è l'angolo tra $0a$ e $0b$ in senso antiorario. L'angolo φ coincide anche con l'argomento del numero complesso $z = b/a$, perciò

$$\sin\varphi = \frac{Im(z)}{|z|} = \frac{z-\overline{z}}{2|z|i} = \frac{(b/a - \overline{b}/\overline{a})|a|}{2|b|i}.$$

Di conseguenza

$$S = \frac{|a|^2 \cdot (b/a - \overline{b}/\overline{a})}{4i} = \frac{\overline{a}b - a\overline{b}}{4i}.$$

Questo è il valore "algebrico" dell'area, che può essere negativo se $\varphi < 0$. Il valore assoluto dell'area è $\frac{|\overline{a}b - a\overline{b}|}{4}$.

2.12

$$\frac{7-6i}{2+3i} = -\frac{4}{13} - i\frac{33}{13}; \qquad \frac{2i}{(2+i)^2} = \frac{8}{25} + i\frac{6}{25}.$$

2.13

$$\frac{2-2i}{3+3i} = -\frac{2}{3}i = \frac{2}{3}\left(\cos\left(\frac{3}{2}\pi\right) + i\,\mathrm{sen}\left(\frac{3}{2}\pi\right)\right);$$

$$-7\sqrt{3} = 7\sqrt{3}(\cos\pi + i\,\mathrm{sen}(\pi));$$

$$(1+i\sqrt{3})^2 = (1-3+i2\sqrt{3}) = 4\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right) = 4\left(\cos\left(\frac{2}{3}\pi\right)+i\,\mathrm{sen}\left(\frac{2}{3}\pi\right)\right).$$

2.15 Per fare questi calcoli ricordiamo che $\cos(\pi/3) + i\,\mathrm{sen}(\pi/3)$ è radice sesta dell'unità, e $\cos(11\pi/6) + i\,\mathrm{sen}(11\pi/6)$ è radice dodicesima dell'unità.

$$(1+i)^{86} = [(1+i)^2]^{43} = (2i)^{43} = -2^{43}i;$$

$$(1+i\sqrt{3})^{42} = [2(\cos(\pi/3)+i\,\mathrm{sen}(\pi/3)]^{42} = 2^{42}[(\cos(\pi/3)+i\,\mathrm{sen}(\pi/3)^6]^7 = 2^{42};$$

$$(\sqrt{3}-i)^{210} = [2(\cos(11\pi/6) + i\,\mathrm{sen}(11\pi/6))]^{210} =$$
$$= 2^{210}[(\cos(11\pi/6) + i\,\mathrm{sen}(11\pi/6)^6]^{35} = 2^{210}(-1)^{35} = -2^{210}.$$

Un modo più veloce di fare questi calcoli è osservando, per esempio, che

$$(1+i\sqrt{3})^3 = 1 + 3\sqrt{3}i - 3\cdot 3 - i3\sqrt{3} = -8,$$

o infine

$$(\sqrt{3}-i)^3 = 3\sqrt{3} - 9i - 3\sqrt{3} - i = 8i.$$

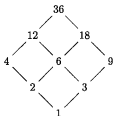
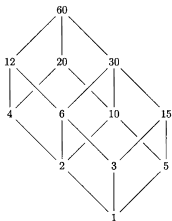
2.16

$$\overline{z} = \rho(\cos(-\varphi) + i\,\mathrm{sen}(-\varphi)) \qquad z^{-1} = \rho^{-1}(\cos(-\varphi) + i\,\mathrm{sen}(-\varphi)).$$

2.17 Sia $z = \rho(\cos(\varphi) + i\,\mathrm{sen}(\varphi)) \in \mathbb{C}$ soluzione dell'equazione $x^4 + i = 0$. Allora

$$\rho^4 = 1,\ \ 4\varphi = 3/2\pi + 2k\pi \implies \rho = 1,\ \ \varphi = 3\pi/8 + k\pi/2, \quad k = 0,1,2,3.$$

2.22 (a) Si applichi la formula del binomio per $(1+i)^{4n}$.

2.24

L'insieme ordinato dei divisori di 36

L'insieme ordinato dei divisori di 60

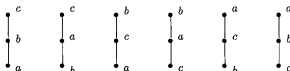
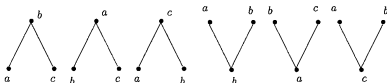
2.25 Siano a, b, c i tre elementi distinti dell'insieme X. Allora i possibili ordini sono:

(1) nessuna coppia di elementi è confrontabile, cioè l'ordine è discreto: dati $x, y \in X$ con $x \neq y$, si ha

$$x \not\leq y \quad \text{e} \quad y \not\leq x;$$

(2) due elementi sono confrontabili e il terzo non lo è con nessuno degli altri due: ci sono 6 ordini di questo tipo

$$b \leq c,\ c \leq b,\ a \leq b,\ b \leq a,\ a \leq c \text{ e } c \leq a:$$

(3) i tre elementi formano una catena; $a \leq b \leq c$, ci sono 6 ordini di questo tipo:

(4) esiste un massimo e l'insieme non è una catena: $a \leq b \geq c$ (ci sono 3 ordini di questo tipo) oppure esiste un minimo e l'insieme non è una catena: $a \geq b \leq c$ (ci sono 3 ordini di questo tipo).

In totale ci sono 19 possibili ordinamenti su un insieme con 3 elementi.

2.26 Diamo un suggerimento. Gli ordini che hanno un elemento massimo o un elemento minimo sono facilmente riducibili all'esercizio 2.25. Resta da determinare il numero degli ordini che non hanno né un elemento massimo né un elemento minimo. Di questo tipo sono tutti gli ordini che hanno un elemento isolato (non confrontabile con gli altri elementi). Infine resta un ultimo tipo di ordine, senza elementi isolati, né minimi né massimi.

13.3 Esercizi del capitolo 3

3.1 Si ha $n \wedge m = (m, n)$ e $n \vee m = m.c.m.(n, m)$ in entrambi casi. $(\mathbb{N}^*, |)$ non è limitato perché non ammette massimo che avevamo dimostrato essere lo zero di $\mathbb{N}$.

3.6 Supponiamo che $p_0 = 2, p_1, p_2, \ldots, p_n$ siano tutti i numeri primi del tipo $3k+2$ e consideriamo il numero $N = 3p_1p_2 \ldots p_n + 2$. Poiché 3 non divide N, i divisori primi di N sono dispari e del tipo $3k+1$ e $3k+2$. Prodotto di numeri del tipo $3k+1$ è dello stesso tipo, quindi almeno uno dei divisori primi q di N è del tipo $3k+2$. Di conseguenza, q coincide con uno dei $p_0, p_1, p_2, \ldots, p_n$ e $q \neq p_0$ perché N è dispari, assurdo, perché nessun p_i può dividere N. Analogamente negli altri casi.

3.9 Osserviamo che $(30, 126) = 6$ divide 42. Pertanto

$$42 = 6 \cdot 7 = (126 - 30 \cdot 4) \cdot 7 \equiv_{126} 30 \cdot (-28),$$

da cui si ricava che le soluzioni sono del tipo $x = -28 + z \cdot 126/6$. Quindi se cerchiamo tutte le soluzioni in $\mathbb{Z}_{126}$, queste sono 14, 35, 56, 77, 98, 119.

3.10 Si vede facilmente che gli interi che soddisfano quella congruenza sono del tipo $x = 36 + 29z$ e pertanto si avrà $x = 7, 36, 65, 94$.

3.15 Notare che $7^4 \equiv_{25} 1$ e $7^4 \equiv_8 1$. Quindi $7^4 \equiv_{100} 1$ e quindi le ultime due cifre di 7^{4k} sono ... 01. Dalla congruenza $7^4 \equiv_{25} 1$ dedurre che $7^{20} \equiv_{125} 1$. Di conseguenza $7^{20} \equiv_{1000} 1$.

3.17 Per verificare che 67 è primo basta controllare che nessun primo p è minore di $\sqrt{67}$, cioè, $p = 2, 3, 5$ e 7 divide 67. Si procede analogamente con 97, 193 e 257.

(a) Da $2^6 \equiv_{67} -3$ ricavare, elevando al quadrato, $2^{12} \equiv_{67} 9$ e $2^{24} \equiv_{67} 14$. Moltiplicando la prima e l'ultima congruenza si ricava $2^{30} \equiv_{67} 25$. Ora moltiplicare per 8 per ottenere $2^{33} \equiv_{67} -1$ e quindi, e $2^{33} \not\equiv_{67} 1$. Per gli altri divisori propri 6 e 22 di 66 abbiamo $2^6 \not\equiv_{67} 1$ e $2^{22} \not\equiv_{67} 1$. D'altra parte, dal lemma 3.35 sappiamo che $o_{67}(2)$ divide 66. Questo permette di scrivere $o_{67}(2) = 66$ perché ogni divisore proprio di 66 divide uno dei divisori 6, 22 e 33.

(b) Da $2^9 \equiv_{97} 27$ e $2^7 \equiv_{97} 31$ ricavare moltiplicando $2^{16} \equiv_{97} 61 \equiv_{97} -36$ e elevando al quadrato $2^{32} \equiv_{97} 35$. Moltiplicando le ultime due congruenze si ottiene $2^{48} \equiv_{97} 1$. Poiché $2^{16} \not\equiv_{97} 1$ e $2^{24} \not\equiv_{97} 1$ (spiegare perché!) si conclude che $o_{97}(2) = 48$.

(c) Per 193 notare che partendo da $2^{10} \equiv_{193} 59$ si ricava $2^{16} \equiv_{193} -84$ e, elevando al quadrato, $2^{32} \equiv_{193} 108$. Moltiplicando le due congruenze si ottiene $2^{48} \equiv_{193} -1$, che permette di affermare $o_{193}(2) = 96$.

(d) Per $257 = 2^8 + 1$ si ha $2^8 \equiv_{257} -1$ e quindi $2^{16} \equiv_{257} 1$. Ora $o_{257}(2) = 16$.

3.18 Si faccia induzione sul numero s di primi che compaiono nella fattorizzazione di n in primi. Se $s = 1$, allora $n = p^k$ e

$$\sum_{d|n} \varphi(d) = \sum_{i=0}^{k} \varphi(p^i) = 1 + \sum_{i=1}^{k} p^{i-1}(p-1) = 1 + (p-1)(1+p+\ldots+p^{k-1}) = p^k.$$

Sia ora $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{k_s}$ e poniamo $m = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_{s-1}^{k_{s-1}}$. Allora i divisori di n sono tutti i divisori di m e poi tutti i divisori del tipo dp_s^i, ove d divide m e $0 < i \leq k_s$. Possiamo applicare l'ipotesi induttiva ad m e quindi

$$\sum_{d|n}\varphi(d)=\sum_{d|m}\varphi(d)+\sum_{d|m}\left(\sum_{i=1}^{k_s}\varphi(dp^i)\right)=$$

$$=m+\sum_{d|m}\left(\sum_{i=1}^{k_s}\varphi(d)\varphi(p^i)\right)=m+\sum_{d|m}\varphi(d)\left(\sum_{i=1}^{k_s}\varphi(p^i)\right)=$$

$$=m+\left(\sum_{d|m}\varphi(d)\right)(p_s^{k_s}-1)=m+m\cdot p_s^{k_s}-m=n.$$

3.19 (a) Se esiste $d \in \mathbb{N}$ con $1 < d < b$ e $d|b$, allora $d < b$ è un divisore proprio di $f_b(d)$, che pertanto non può essere un primo.

(b) Le prime verifiche sono immediate, per $b = 17$ si utilizzi l'esercizio 3.4 e per $b = 41$ si facciano le opportune verifiche.

(c) Supponiamo $b \geq 7$. Notiamo che per $x = 2, 3, 4, 5, 6$, si ha

$$x(x-1) = 2, 6, 12, 20, 30$$

rispettivamente. Se

$$f_b(x) = x^2 - x + b = x(x-1) + b$$

è un polinomio di Eulero, allora per il punto (a), b è un primo. Inoltre da quanto appena osservato e dalla definizione si ha che anche $b+2$, $b+6$, $b+12$, $b+20$ e $b+30$ devono essere dei primi. Quindi in particolare b deve essere il più piccolo di una coppia di primi gemelli. Osserviamo che, poiché b è un primo, $b \equiv_6 1$ o 5. Ma se fosse $b \equiv_6 1$, allora $b+2 \equiv_6 3$ e quindi $b+2$ sarebbe divisibile per 3 e non potrebbe essere un primo.

Vediamo quale può essere l'ultima cifra di b. Se fosse $b \equiv_{10} 5$, b sarebbe divisibile per 5 e quindi non potrebbe essere un primo. Se fosse $b \equiv_{10} 3$, $b+2$ sarebbe divisibile per 5 e infine $b \equiv_{10} 9$, $b+6$ sarebbe divisibile per 5, in contraddizione con quanto richiesto.

Concludendo abbiamo $b \equiv_6 5$ e $b \equiv_{10} 1$ oppure 7. Questo ci permette di concludere allora che b deve essere del tipo $b = 11 + 30k$ oppure $b = 17 + 30k$. Gli unici possibili primi che dobbiamo indagare sono: $b = 11, 17, 41, 47, 71, 77$ se vogliamo fermarci a 100. Ma 77 non è un primo, e 47 non è un primo gemello, infatti 49 non è primo. Per quel che riguarda 71, osserviamo che 71+2= 73 è un primo, ma 71+6=77 non lo è già più. Se vogliamo continuare fino a 1000, è facile scrivere tutti i numeri del tipo descritto e poi basta avere sottomano una lista dei primi minori di 1000 per controllare che gli unici primi della forma $b = 11 + 30k$ oppure $b = 17 + 30k$ con $b+2$ primo sono b =101, 107, 137, 191, 197, 227, 281, 347, 431, 461, 491, 521, 617, 641, 821, 827, 857, 881. Per questi, un facile controllo mostra che almeno uno dei $b+6$, $b+12$, $b+20$, $b+30$, $b+42$ o $b+72$ non è un primo.

3.20 Se $m = q \cdot r$, dove $r > 1$ è un divisore dispari di m, allora

$$2^{qr} + 1 = (2^q + 1)(2^{q(r-1)} - \cdots + 1)$$

e

$$1 < 2^q + 1 < 2^m + 1,$$

quindi $2^m + 1$ non può essere primo. Non avendo m dei divisori dispari concludiamo che $m = 2^n$ per qualche numero naturale n.

3.22 (a) Basta eseguire il prodotto di destra e osservare che si cancellano tutti i termini, eccetto il primo e l'ultimo.

(b) Se $m|n$, allora $n = mq$, pertanto

$$(x^n - 1) = ((x^m)^q - 1) = (x^m - 1)((x^m)^{n-1} + \ldots + x^m + 1)$$

per il punto (a). Da questo si vede che $(x^m - 1)$ divide $(x^n - 1)$.

(c) Se $x > 2$, allora $x^m - 1 = (x-1)(x^{r-1} + \cdots + x + 1)$ per il punto (a), e quindi è divisibile per $x - 1$. Se d divide m allora $x^d - 1$ divide $x^m - 1$ per il punto (b).

3.24 Poiché $2^{p-1} \equiv_p 1$ per il piccolo teorema di Fermat e $2^n \equiv_p 1$ per ipotesi, si ha che n divide $p - 1$ poiché n è primo.

3.25 Per l'esercizio 3.24 ogni divisore primo p di M_{13} è del tipo $p = 13k + 1$. In più essendo p dispari, si avrà anche $p = 26k + 1$, in altre parole k può essere solo pari. D'altra parte, $M_{13} < 91^2$, quindi $p \leq 89$ e quindi $k = 1, 2, 3$ sono gli unici possibili valori di k. Per $k = 1$ risulta $p = 27$ non primo. Resta da verificare che 53 e 79 non dividono M_{13}.

3.28 Usare l'esercizio 3.56 (c) per il primo 5.

3.31 Supponiamo per assurdo che ci sia un numero finito di numeri primi del tipo $4k+1$ e li elenchiamo: $p_1, p_2, \ldots, p_n$. Sia ora $N = 4(p_1p_2\ldots p_n)^2 + 1$. Per la nostra ipotesi N non può essere primo essendo maggiore di tutti i p_k. Sia p un divisore primo di N. Allora, per l'esercizio 3.32, p deve essere della forma $4k+1$ e coincidere con qualche p_k, assurdo perché nessun p_k divide N. Similmente per i primi del tipo $8k + 1$.

3.32 (a) Essendo p dispari, per $t = \frac{p-1}{2}$ abbiamo $1 \equiv_p a^{p-1} = (a^2)^t \equiv_p (-1)^t$, quindi $(-1)^t = 1$ e di conseguenza $t = 2k$ è pari. Questo dimostra $p = 4k + 1$.

(b) Dal punto (a) applicato ad a^2 concludiamo che $p = 4t + 1$ per qualche $t \in \mathbb{Z}$. Sia $t = \frac{p-1}{4}$. Allora $1 \equiv_p a^{p-1} = (a^4)^t \equiv_p (-1)^t$, quindi $(-1)^t = 1$ e di conseguenza $t = 2k$. Questo dimostra $p = 8k + 1$.

3.35 Lo dimostriamo usando il principio di induzione nella seconda forma. Se $n = 1$ allora basterà prendere $c_1 = 1$. Sia ora n un numero naturale e sia m il massimo dei naturali tali che $m! \leq n$, allora $(m+1)! > n$. Grazie alla divisione euclidea di n per $m!$, esistono $q, r \in \mathbb{N}$, con $0 \leq r < m!$ tali che $n = q \cdot m! + r$. Applichiamo ora a $r < m! \leq n$ l'ipotesi induttiva. Otteniamo $r = \Sigma_{i=1}^{r} c_i \cdot i!$, con $0 \leq c_i \leq i$. Poiché $r < m!$, la sommatoria precedente si arresta ad $m - 1$, cioè $r = \Sigma_{i=1}^{m-1} c_i \cdot i!$, con $0 \leq c_i \leq i$. Pertanto

$$n = q \cdot m! + r = q \cdot m! + \Sigma_{i=1}^{m-1} c_i \cdot i! = \Sigma_{i=1}^{m} c_i \cdot i!$$

ponendo $q = c_m$ ed osservando che $0 \leq q = c_m \leq m$, cioè $q < m + 1$. Infatti $(m+1)m! = (m+1)! > n = q \cdot m! + r \geq q \cdot m!$, da cui dividendo per $m!$, si ottiene $q < m + 1$.

3.43 Sia $d = (x^m - 1, x^n - 1)$ e sia $c = (m, n)$. Poiché c divide sia m che n, avremo che $x^c - 1$ divide sia $(x^m - 1)$ che $(x^n - 1)$ per il punto b) dell'esercizio 3.22. Pertanto $x^c - 1$ divide anche d.

Poiché $c = (m, n)$, esistono $u, v \in \mathbb{N}$ tali che $c = mu - nv$. Allora d divide $x^m - 1$ e quindi divide anche $x^{mu} - 1$ e analogamente d divide $x^{nv} - 1$. Allora d divide anche la loro differenza, cioè d divide

$$(x^{mu} - 1) - (x^{nv} - 1) = x^{mu} - x^{nv} = x^{nv}(x^{mu-nv} - 1).$$

Poiché $x^m - 1$ e x sono due numeri naturali coprimi, e d divide $x^m - 1$, si avrà che d è coprimo con x^{nv} e quindi divide

$$(x^{mu-nv} - 1) = x^c - 1.$$

3.52 Notare che $\varphi(n)$ divide $n!$.

3.56 (a) Sfruttare la formula $C_k^p = \frac{p!}{k!(p-k)!}$ e il fatto che p divide il numeratore ed è coprimo con il denominatore.

(b) Segue da (a) per induzione su s.

(c) $\left\lfloor \frac{n}{p} \right\rfloor$ coincide con il numero dei multipli di p nel prodotto che definisce $n!$. Di questi $\left\lfloor \frac{n}{p^2} \right\rfloor$ sono multipli di p^2, e contribuiscono ciascuno con un altro fattore p, $\left\lfloor \frac{n}{p^3} \right\rfloor$ sono multipli di p^3, e contribuiscono ciascuno con un altro fattore p, ecc.

3.57 Usare l'esercizio 3.56 (c).

13.4 Esercizi del capitolo 4

4.1 Fissare $n \in \mathbb{N}$ arbitrariamente e dimostrare per induzione su m che vale per tutti gli $m \in \mathbb{N}$

$$x^{n+m} = x^n x^m.$$

4.7 Sia S semigruppo finito ed $x \in S$. Poiché S è finito, l'insieme $\{x^n : n \in \mathbb{N}_+\}$ finito. Allora esistono $i, j \in \mathbb{N}_+$ tali che $i \neq j$ e $x^i = x^j$. Possiamo supporre $i >$ allora $x^j = x^i = x^{i-j} x^j$. Proviamo per induzione su n che

$$x^j = x^{n(i-j)} x^j$$

per ogni $n \in \mathbb{N}_+$. Il caso $n = 1$ lo abbiamo già provato. Supponiamolo vero per $n - 1 \geq 1$ e proviamolo per n:

$$x^j = x^{(n-1)(i-j)}x^j = x^{(n-1)(i-j)}x^i = x^{(n-1)(i-j)}x^{i-j}x^j = x^{n(i-j)}x^j.$$

Allora esiste $k \in \mathbb{N}$ tale che $k(i-j) > j$. Quindi

$$x^{k(i-j)}x^{k(i-j)} = x^{k(i-j)}x^{k(i-j)-j+j} = x^{k(i-j)}x^j x^{k(i-j)-j} =$$
$$= x^j x^{k(i-j)-j} = x^{k(i-j)},$$

cioè $x^{k(i-j)}$ è idempotente.

4.8 Si applichino l'esercizio 4.7 ed il lemma 4.6 per dedurre che S è un monoide e si utilizzi il teorema 4.13 per concludere.

4.9 Per l'esercizio 4.7, S ha sempre un idempotente, quindi deve valere $a^2 = a$ oppure $b^2 = b$ in ogni tabella. Questo elimina le quattro tabelle con $a^2 = b$ e $b^2 = a$. Inoltre se vale $b^2 = a$, allora il semigruppo è abeliano. Infatti, se avessimo $ab = b$ e $ba = a$, allora $(ba)b = ab = b$, mentre $b(ab) = b^2 = a$ e quindi non varrebbe la legge associativa. In questo modo sono state eliminate altre 4 tabelle. Visto che ci sono 16 applicazioni distinte $S \times S \to S$, restano 8 tabelle che riportiamo qui sotto. Lasciamo al lettore la verifica che esse definiscono una struttura di semigruppo su S. Ci sono essenzialmente 4 strutture diverse – la prima, la seconda, la terza e la quarta, che risulta l'unica non abeliana. Le altre 4 strutture si ricavano scambiando semplicemente a e b. Le tabelle 1 e 5 presentano le due strutture in cui la moltiplicazione è una funzione costante su $S \times S$.

Tabella 1

·	a	b
a	a	a
b	a	a

Tabella 2

·	a	b
a	b	a
b	a	b

Tabella 3

·	a	b
a	a	b
b	b	b

Tabella 4

·	a	b
a	a	a
b	b	b

Tabella 5

·	a	b
a	b	b
b	b	b

Tabella 6

·	a	b
a	a	b
b	b	a

Tabella 7

·	a	b
a	a	a
b	a	b

Tabella 8

·	a	b
a	a	b
b	a	b

4.10 (a) Si verifica facilmente che $|$ soddisfa la proprietà riflessiva e transitiva.

(b) Proviamo che $|$ soddisfa anche la proprietà antisimmetrica. Siano $a, b \in S$ tali che $a|b$ e $b|a$. Allora esistono $x, y \in S$ tali che $a = by$ e $b = ax$. Poichè

$$b1 = b = ax = (by)x = b(yx) \quad \text{e} \quad a1 = a = by = (ax)y = a(xy),$$

la legge di cancellazione valida in S implica che $yx = 1 = xy$. Per l'unicità dell'inverso si ha $y = x = 1$ e dunque $a = b$.

Poiché $a = a1$ per ogni $a \in S$, risulta $1|a$ per ogni $a \in S$ e dunque 1 è l'elemento minimo cercato.

4.11 È facile verificare che $(\mathbb{Q} \times \mathbb{Z}^*, \cdot)$ è un monoide con elemento neutro $(0, 1)$. Un elemento $(q, m) \in \mathbb{Q} \times \mathbb{Z}^*$ è invertibile se e solo se esiste $(q', m') \in \mathbb{Q} \times \mathbb{Z}^*$ tale che

$$(q, m) \cdot (q', m') = (q + mq', mm') = (0, 1) = (q' + m'q, m'm) = (q', m') \cdot (q, m).$$

Ciò accade se e solo se $q + mq' = 0 = q' + m'q$ e $mm' = 1$ se e solo se $m = m' = 1$ e $q + q' = 0$ oppure $m = m' = -1$ e $q - q' = 0$. Quindi gli elementi invertibili di $\mathbb{Q} \times \mathbb{Z}^*$ sono tutti e soli della forma $(q, 1)$, con inverso $(-q, 1)$ e $(q, -1)$, con inverso $(q, -1)$. Infine $(\mathbb{Q} \times \mathbb{Z}^*, \cdot)$ non è abeliano perché presi gli elementi $(q, m), (q', m) \in \mathbb{Q} \times \mathbb{Z}^*$ con $q \neq q'$ e $m \neq 1$, non commutano.

4.12 $(\{0\}, +)$, $(\{1, -1\}, \cdot)$ e $(\mathbb{Q}_+, \cdot)$ sono gruppi mentre $(\{0, 1\}, \cdot)$ non lo è poiché l'elemento 0 non ammette inverso.

4.14 È facile verificare che $(\mathbb{Q}^* \times \mathbb{Q}, \cdot)$ è un monoide con elemento neutro $(1, 0)$. Inoltre per ogni $(a, b) \in \mathbb{Q}^* \times \mathbb{Q}$ l'elemento $(a^{-1}, -b)$ appartiene a $\mathbb{Q}^* \times \mathbb{Q}$ e

$$(a^{-1}, -b) \cdot (a, b) = (1, 0) = (a, b) \cdot (a^{-1}, -b).$$

Quindi $(\mathbb{Q}^* \times \mathbb{Q}, \cdot)$ è un gruppo. Non è abeliano perché presi $(a, b), (a, b') \in \mathbb{Q}^* \times \mathbb{Q}$ con $a \neq \pm 1$ e $b \neq b'$,

$$(a, b) \cdot (a, b') \neq (a, b') \cdot (a, b).$$

4.16 Siano $f \in G$ e $x, y \in \mathbb{R}$. Allora $f(x) = f(y)$ se e solo se $ax + b = ay + b$ se e solo se $ax = ay$ se e solo se $x = y$ poiché $a \neq 0$. Dunque f è iniettiva. Inoltre f è anche suriettiva poiché per ogni $y \in \mathbb{R}$ si ha $y = f\left(\frac{y-b}{a}\right)$. Ciò prova che $G \subseteq S_{\mathbb{R}}$. Siano $f, g \in G$ tali che $f(x) = ax + b$ e $g(x) = cx + d$ per ogni $x \in \mathbb{R}$ con $a, c \in \mathbb{R} \setminus \{0\}$ e $b, d \in \mathbb{R}$. Allora $(g \circ f)(x) = g(ax + b) = cax + cb + d$ per ogni $x \in \mathbb{R}$ e quindi $g \circ f \in G$ poiché $ac \neq 0$. È facile verificare che $(G, \circ)$ è un monoide con elemento neutro $id_{\mathbb{R}}$ e che ogni $f \in G$ è invertibile con inversa definita da $f^{-1}(x) = a^{-1}x - \frac{b}{a}$ per ogni $x \in \mathbb{R}$. Ciò prova che $(G, \circ)$ è un gruppo. Infine G non è abeliano perché date f e g definite rispettivamente da

$$x \mapsto 2x + 5 \quad \text{e} \quad x \mapsto 3x + 1,$$

si ha $g \circ f \neq f \circ g$.

4.17 Innanzitutto U è non vuoto poiché $1 \in U$. Inoltre $u^{-1} \in U$ per ogni $u \in U$. Per concludere si osservi che se $u, v \in U$, allora

$$(uv)(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = uu^{-1} = 1 =$$

$$= v^{-1}v = v^{-1}(u^{-1}u)v = (v^{-1}u^{-1})(uv).$$

Quindi $uv \in U$.

4.19 Considerare l'insieme X di tutte le famiglie linearmente indipendenti $\mathcal{V}$ di vettori di V e ordinare X con l'inclusione. Dimostrare che $(X, \subseteq)$ è induttivo e applicare il lemma di Zorn per ottenere una famiglia massimale $\mathcal{M}$. Dimostrare che $\mathcal{M}$ risulta una base. Sia $\mathcal{B}$ un altra base di V. Ogni elemento $b \in \mathcal{B}$ determina univocamente un sottoinsieme $f(b)$ di $\mathcal{M}$ che lo genera. In questo modo si definisce un'applicazione $\varphi : \mathcal{B} \to \mathcal{P}_\infty(\mathcal{M})$, dove $\mathcal{P}_\infty(\mathcal{M})$ denota la famiglia dei sottoinsiemi finiti di $\mathcal{M}$. Essendo b contenuto nel sottospazio generato da $f(b)$ di dimensione $|f(b)|$, l'antimmagine di ogni $F \in \mathcal{P}_\infty(\mathcal{M})$ può avere al più dim F elementi. Quindi esiste un'iniezione da $\varphi^{-1}(F)$ in $\mathbb{N}$ per ogni $F \in \mathcal{P}_\infty(\mathcal{M})$. Poiché

$$\mathcal{B} = \bigcup_{F \in \mathcal{P}_\infty(\mathcal{M})} \varphi^{-1}(F)$$

per l'esempio 1.48, possiamo costruire una iniezione da $\mathcal{B}$ in $\mathcal{P}_\infty(\mathcal{M}) \times \mathbb{N}$. Poiché $|\mathcal{P}_\infty(\mathcal{M}) \times \mathbb{N}| = |\mathcal{P}_\infty(\mathcal{M})|$ per il teorema 1.79, abbiamo così dimostrato che $|\mathcal{B}| \leq |\mathcal{P}_\infty(\mathcal{M})|$. Si dimostra facilmente che $\mathcal{P}_\infty(\mathcal{M})$ è equipotente a $\mathcal{M}$, basta notare che

$$\mathcal{P}_\infty(\mathcal{M}) = \bigcup_{n=1}^{\infty} \mathcal{P}_n(\mathcal{M}),$$

dove $\mathcal{P}_n(\mathcal{M})$ denota la famiglia dei sottoinsiemi finiti di $\mathcal{M}$ con esattamente n elementi, e

$$|\mathcal{P}_n(\mathcal{M})| \leq |\mathcal{M}|^n = |\mathcal{M}|$$

per il lemma 1.80 e per induzione su n. Questo dimostra che $|\mathcal{B}| \leq |\mathcal{M}|$. Scambiando i ruoli di $\mathcal{B}$ ed $\mathcal{M}$ proviamo anche $|\mathcal{M}| \leq |\mathcal{B}|$.

4.20 Considerare $\mathbb{R}^\mathbb{N}$ come spazio vettoriale sopra $\mathbb{R}$.

13.5 Esercizi del capitolo 5

5.1 Dimostriamo che l'ordine di ab divide mn. Per il lemma 5.3 risulta

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1^n 1^m = 1$$

e la tesi segue dal punto (a) del lemma 5.5.

5.4 Si consideri un ciclo di lunghezza pari.

5.7 La decomposizione di σ in cicli disgiunti è $\sigma = (1\ 5\ 12)(2\ 6\ 9\ 11)(3\ 7\ 4\ 10\ 8)$. Siano $\tau_1 := (1\ 5\ 12)$, $\tau_2 := (2\ 6\ 9\ 11)$ e $\tau_3 := (3\ 7\ 4\ 10\ 8)$. Allora per il lemma 5.3 risulta che

$$\sigma^n = \tau_1^n \tau_2^n \tau_3^n$$

per ogni $n \in \mathbb{Z}$. Osserviamo che:
$\tau_1^3 = id \Longrightarrow \tau_1^2 = \tau_1^{-1}$;

$\tau_2^4 = id \Longrightarrow \tau_2^3 = \tau_2^{-1}$ e $\tau_2^5 = \tau_2$;
$\tau_3^5 = id \Longrightarrow \tau_3^3 = \tau_3^{-2}$.
Quindi

$$\sigma^2 = (1\ 12\ 5)(2\ 9)(6\ 11)(3\ 4\ 8\ 7\ 10);$$

$$\sigma^3 = (2\ 11\ 9\ 6)(3\ 10\ 7\ 8\ 4) \quad \text{e} \quad \sigma^5 = (1\ 12\ 5)(2\ 6\ 9\ 11).$$

5.11 Come si è visto nel lemma 5.31, $\langle X \rangle$ è un sottogruppo e quindi $x^n, y^m \in \langle X \rangle$ per ogni $n, m \in \mathbb{Z}$. Si può dimostrare per induzione su k che

$$x^{n_1} y^{m_1} x^{n_2} y^{m_2} \dots x^{n_k} y^{m_k} \in \langle X \rangle,$$

per ogni $k \in \mathbb{N}_+, n_i, m_i \in \mathbb{Z}$. Pertanto l'insieme H è contenuto in $\langle X \rangle$. Per l'altra inclusione basta vedere che H è un sottogruppo. Infatti, se

$$x^{n_1} y^{m_1} x^{n_2} y^{m_2} \dots x^{n_k} y^{m_k}, \quad x^{i_1} y^{j_1} x^{i_2} y^{j_2} \dots x^{i_h} y^{j_h} \in H,$$

allora

$$x^{n_1} y^{m_1} x^{n_2} y^{m_2} \dots x^{n_k} y^{m_k} x^{i_1} y^{j_1} x^{i_2} y^{j_2} \dots x^{i_h} y^{j_h} \in H.$$

Inoltre

$$(x^{n_1} y^{m_1} x^{n_2} y^{m_2} \dots x^{n_k} y^{m_k})^{-1} = y^{-m_k} x^{-n_k} \dots y^{-m_1} x^{-n_1} =$$

$$= x^0 y^{-m_k} x^{-n_k} \dots y^{-m_1} x^{-n_1} y^0$$

che è ancora un elemento di H.

La seconda affermazione segue dal fatto che, se x, y commutano, allora

$$x^{n_1} y^{m_1} x^{n_2} y^{m_2} \dots x^{n_k} y^{m_k} = x^{n_1+n_2 \dots + n_k} y^{m_1+m_2 \dots + m_k}.$$

5.12 Definiamo

$$\mathcal{H} := \{h_1 k_1 h_2 k_2 \dots h_s k_s : s \in \mathbb{N}_+, h_i \in H, k_i \in K \text{ per } i = 1, 2, \dots, s\}.$$

Poiché $\langle X \rangle$ è un sottogruppo di G contenente H e K, $\langle X \rangle$ contiene anche i prodotti dei loro elementi e quindi $hk \in \langle X \rangle$ per ogni $h \in H$ e $k \in K$. Sfruttando (S1) della definizione di sottogruppo si può dimostrare per induzione su $s \in \mathbb{N}_+$ che $\mathcal{H} \subseteq \langle X \rangle$. Chiaramente $\mathcal{H}$ contiene sia H che K, poiché $h = h1$ per ogni $h \in H$ e $k = 1k$ per ogni $k \in K$.

Per dimostrare l'inclusione $\langle X \rangle \subseteq \mathcal{H}$ basta quindi verificare che $\mathcal{H}$ è un sottogruppo di G. Infatti, se

$$h_{i_1} k_{i_1} h_{i_2} k_{i_2} \dots h_{i_s} k_{i_s}, \quad \text{e} \quad h_{j_1} k_{j_1} h_{j_2} k_{j_2} \dots h_{j_t} k_{j_t} \in \mathcal{H},$$

allora

$$h_{i_1} k_{i_1} h_{i_2} k_{i_2} \dots h_{i_s} k_{i_s} h_{j_1} k_{j_1} h_{j_2} k_{j_2} \dots h_{j_t} k_{j_t} \in \mathcal{H}.$$

Inoltre

$$(h_{i_1}k_{i_1}h_{i_2}k_{i_2}\dots h_{i_s}k_{i_s})^{-1} = 1k_{i_s}^{-1}h_{i_s}^{-1}\dots k_{i_1}^{-1}h_{i_1}^{-1}1 \in \mathcal{H}.$$

La seconda affermazione segue dal fatto che, se G è abeliano, allora gli elementi di H e K permutano e quindi $h_{i_1}k_{i_1}h_{i_2}k_{i_2}\dots h_{i_s}k_{i_s} = hk$ ove

$$h = h_{i_1}h_{i_2}\dots h_{i_s} \in H \quad \text{e} \quad k = k_{i_1}k_{i_2}\dots k_{i_s} \in K.$$

5.14 Sia $V = \{(12)(34), (13)(24), (14)(23), id\}$. Essendo prodotto di trasposizioni disgiunte, ogni permutazione σ di V ha periodo 2. Quindi $\sigma = \sigma^{-1}$ e V contiene dunque gli inversi di ogni suo elemento. È facile verificare che $\sigma \circ \tau \in V$ per ogni coppia di permutazioni $\sigma, \tau \in V$.

5.16 (a) Osserviamo che $id_{\mathbb{R}} \in \mathcal{C}(\mathbb{R})$. Inoltre poiché la differenza di funzioni continue è ancora un funzione continua, si ha che $f - g \in \mathcal{C}(\mathbb{R})$ per ogni $f, g \in \mathcal{C}(\mathbb{R})$. Per il lemma 5.29 possiamo concludere che $\mathcal{C}(\mathbb{R})$ è un sottogruppo di G.

(b)–(c) Si ragioni come in (a).

5.19 Poiché V è un gruppo abeliano, le classi laterali destre e sinistre di W coincidono. Si osservi che ogni vettore $v \in V$ si rappresenta come $v = le_1 + se_2 + re_3$ ove $l, s, r \in \mathbb{R}$. Quindi $W + v = W + re_3$.

5.20 Sia k la dimensione di W. Si scelga una base $e_1, \dots, e_n$ di V tale che $e_1, \dots, e_k$ sia una base di W e si ragioni come nell'esercizio 5.19.

5.21 Poiché $(\mathbb{Z}, +)$ è un gruppo abeliano, le classi laterali destre e sinistre di un sottogruppo $H \leq \mathbb{Z}$ coincidono. Dato $n \in \mathbb{N}$, un sistema di rappresentanti delle classi laterali del sottogruppo $n\mathbb{Z}$ di $(\mathbb{Z}, +)$ è

$$0 + n\mathbb{Z},\ 1 + n\mathbb{Z},\ 2 + n\mathbb{Z},\ \dots, (n-2) + n\mathbb{Z},\ (n-1) + n\mathbb{Z}$$

e quindi $[\mathbb{Z} : n\mathbb{Z}] = n$.

5.22 Ragionando come nell'esempio 5.59, si verifica che gli unici sottogruppi di $(\mathbb{Z}_2, +)$, $(\mathbb{Z}_3, +)$, $(\mathbb{Z}_5, +)$ e $(\mathbb{Z}_7, +)$ sono $\{0\}$ e G.

Se H è un sottogruppo di $(\mathbb{Z}_8, +)$, allora $|H|$ deve dividere 8 per il teorema di Lagrange. Quindi le sole possibilità sono $|H| = 1, 2, 4, 8$. Si verifica che se H è uno dei sottogruppi

$$\langle [1]_8 \rangle, \quad \langle [3]_8 \rangle, \quad \langle [5]_8 \rangle, \quad \langle [7]_8 \rangle,$$

allora $H = \mathbb{Z}_8$.

Sia $H = \langle [4]_8 \rangle$. Allora $H = \{[0]_8, [4]_8\}$ e quindi $[G : H] = 4$. Un sistema di rappresentanti per le classi laterali di H in G è

$$[0]_8 + H, \qquad [1]_8 + H = \{[1]_8, [5]_8\},$$

$$[2]_8 + H = \{[2]_8, [6]_8\}, \qquad [3]_8 + H = \{[3]_8, [7]_8\}.$$

Sia $K = \langle [2]_8 \rangle$. Allora $K = \{[0]_8, [2]_8, [4]_8, [6]_8\}$ e quindi $[G : K] = 2$. Un sistema di rappresentanti per le classi laterali di K in G è

$$[0]_8 + K, \qquad [1]_8 + K = \{[1]_8, [3]_8, [5]_8, [7]_8\}.$$

Si ragioni in maniera analoga per $(\mathbb{Z}_9, +)$ e $(\mathbb{Z}_{10}, +)$.

5.26 Poiché $|S_3| = 6$, un sottogruppo H di S_3 può avere ordine $1, 2, 3, 6$. Siano $\tau_1 = (23)$, $\tau_2 = (13)$, $\tau_3 = (12)$ e $\sigma = (123)$. Si verifica che $\langle \tau_i, \tau_j \rangle = S_3$ se $i \neq j$ e $\langle \tau_i, \sigma \rangle = S_3$ per ogni $i = 1, 2, 3$. Quindi gli unici sottogruppi propri di S_3 sono $\langle \tau_i \rangle$ per $i = 1, 2, 3$ e $\langle \sigma \rangle$.

5.28 (a) L'elemento $(1, 0)$ è l'unità di G poiché

$$(1, 0) \cdot (a, b) = (1a, 1b + 0) = (a, b) = (a1, a0 + b) = (a, b) \cdot (1, 0)$$

per ogni $(a, b) \in G$.

Se $(a, b) \in G$, allora anche $(a^{-1}, -ba^{-1})$ è un elemento ben definito di G e

$$(a, b) \cdot (a^{-1}, -ba^{-1}) = (1, 0) = (a^{-1}, -ba^{-1}) \cdot (a, b);$$

quindi $(a^{-1}, -ba^{-1}) = (a, b)^{-1}$.

(b) Chiaramente $H \neq \emptyset$ poiché $(1, 0) \in H$. Inoltre, se $(a, 0), (b, 0) \in H$, allora $(a, 0)^{-1} \cdot (b, 0) = (a^{-1}b, 0) \in H$, quindi H è un sottogruppo di G per il lemma 5.29.

5.29 Sia $G = \mathbb{R} \times \mathbb{R}$, $H = \mathbb{R} \times \{0\}$, $K = \{0\} \times \mathbb{R}$ e $L = \{(r, r) : r \in \mathbb{R}\}$ il sottogruppo diagonale. Allora $H + K = G$, mentre $H \cap L = K \cap L = \{0\}$.

5.30 Basta osservare che per due sottogruppi H e K l'estremo superiore $H \vee K$ coincide con $\langle H, K \rangle$ e l'estremo inferiore $H \wedge K$ coincide con $H \cap K$.

5.32 (a) Per definizione un gruppo G è abeliano se e solo se $gx = xg$ per ogni $x, g \in G$ se e solo se $g \in Z(G)$ per ogni $g \in G$ se e solo se $G = Z(G)$.

(b) Per il lemma 5.72 $Z(G)$ è un sottogruppo normale abeliano di G, quindi la semplicità di G implica che $Z(G) = 1$ oppure $Z(G) = G$. Essendo G non abeliano, si conclude che $Z(G) = 1$.

5.37 (a) Per il lemma 5.83 (b) applicato al caso $n = 2$ e $p = 3$ si ottiene

$$|GL_2(\mathbb{F}_3)| = (3^2 - 1)(3^2 - 3) = 48.$$

(b) Sia

$$\mathcal{Z} := \left\{ \begin{pmatrix} [1]_3 & [0]_3 \\ [0]_3 & [1]_3 \end{pmatrix}, \begin{pmatrix} [2]_3 & [0]_3 \\ [0]_3 & [2]_3 \end{pmatrix} \right\}$$

e proviamo che $Z(G) = \mathcal{Z}$. L'inclusione $\mathcal{Z} \subseteq Z(G)$ è ovvia.

Sia $\begin{pmatrix} [a]_3 & [b]_3 \\ [c]_3 & [d]_3 \end{pmatrix} \in Z(G)$ arbitraria e proviamo che $[b]_3 = [c]_3 = [0]_3$. Infatti, data la matrice $\begin{pmatrix} [1]_3 & [0]_3 \\ [0]_3 & [2]_3 \end{pmatrix} \in GL_2(\mathbb{F}_3)$, la condizione

$$\begin{pmatrix} [a]_3 & [2]_3[b]_3 \\ [c]_3 & [2]_3[d]_3 \end{pmatrix} = \begin{pmatrix} [a]_3 & [b]_3 \\ [c]_3 & [d]_3 \end{pmatrix} \begin{pmatrix} [1]_3 & [0]_3 \\ [0]_3 & [2]_3 \end{pmatrix} =$$

$$= \begin{pmatrix} [1]_3 & [0]_3 \\ [0]_3 & [2]_3 \end{pmatrix} \begin{pmatrix} [a]_3 & [b]_3 \\ [c]_3 & [d]_3 \end{pmatrix} = \begin{pmatrix} [a]_3 & [b]_3 \\ [2]_3[c]_3 & [2]_3[d]_3 \end{pmatrix}$$

implica che $[b]_3 = [2]_3[b]_3$ e $[c]_3 = [2]_3[c]_3$, ma questo accade se e solo se

$$[b]_3 = [c]_3 = [0]_3.$$

Proviamo ora che $[a]_3 = [d]_3$. Infatti, data la matrice $\begin{pmatrix} [1]_3 & [0]_3 \\ [1]_3 & [1]_3 \end{pmatrix} \in GL_2(\mathbb{F}_3)$, la condizione

$$\begin{pmatrix} [a]_3 & [0]_3 \\ [d]_3 & [d]_3 \end{pmatrix} = \begin{pmatrix} [a]_3 & [0]_3 \\ [0]_3 & [d]_3 \end{pmatrix} \begin{pmatrix} [1]_3 & [0]_3 \\ [1]_3 & [1]_3 \end{pmatrix} = \begin{pmatrix} [1]_3 & [0]_3 \\ [1]_3 & [1]_3 \end{pmatrix} \begin{pmatrix} [a]_3 & [0]_3 \\ [0]_3 & [d]_3 \end{pmatrix} = \begin{pmatrix} [a]_3 & [0]_3 \\ [a]_3 & [d]_3 \end{pmatrix}$$

implica che $[a]_3 = [d]_3$. Poiché $\det \begin{pmatrix} [a]_3 & [0]_3 \\ [0]_3 & [a]_3 \end{pmatrix} = [1]_3, [2]_3$, si ha che $[a]_3 = [1]_3$ oppure $[a]_3 = [2]_3$.

(c) Si considerino i sottogruppi ciclici di $GL_2(\mathbb{F}_3)$ generati rispettivamente dalle matrici $\begin{pmatrix} [1]_3 & [0]_3 \\ [1]_3 & [1]_3 \end{pmatrix}$ e $\begin{pmatrix} [1]_3 & [1]_3 \\ [0]_3 & [1]_3 \end{pmatrix}$.

5.38 (a) Sia $Z = Z(G)$ ed $a \in G$. Poiché a commuta con ogni elemento di Z, si ha che

$$H := \langle a, Z \rangle = \{a^n z : n \in \mathbb{Z},\ z \in Z\}.$$

Siano $x, y \in H$. Allora esistono $n, m \in \mathbb{Z}$ e $z, z_1 \in Z$ tali che $x = a^n z$ e $y = a^m z_1$. Supponiamo $n \geq m$. Allora

$$xy = a^n z a^m z_1 = a^m a^{n-m} z z_1 a^m = a^m a^{n-m} z_1 z a^m =$$

$$= a^m z_1 a^{n-m} a^m z = a^m z_1 a^n z = yx.$$

Per l'arbitrarietà degli elementi x, y scelti in H, possiamo concludere che H è abeliano.

(b) Se $ab \in Z$, allora $(ab)b = b(ab) = (ba)b$ e quindi $ab = ba$ per la legge di cancellazione valida in G.

(c) Siano $a = (12)$ e $b = (34)$ due elementi del gruppo S_4. Essendo trasposizioni disgiunte, si ha che $ab = ba$. Tuttavia, scelto $c = (13) \in S_4$, si ha che $c(ab) = (1234)$ mentre $(ab)c = (1432)$. Quindi $ab \notin Z(S_4)$ (si veda anche l'esercizio 5.39).

5.39 (a) Poiché $S_2 \cong \mathbb{Z}_2$, $Z(S_2) = S_2$.

(b) Osserviamo che se a, b sono due elementi di un gruppo G tali che $ab \neq ba$, allora $a, b \notin Z(G)$. Poiché $Z(G)$ è un sottogruppo normale di G segue che anche $a^{-1}, b^{-1}, (ab)a^{-1} \notin Z(G)$. Inoltre per l'esercizio 5.38 (b), anche $ab, ba \notin Z(G)$.

Siano a, b rispettivamente gli elementi (12) e (23) di S_3. Poiché

$$ab = (123) \neq (132) = ba$$

e

$$(ab)a^{-1} = (13),$$

per quanto appena osservato possiamo concludere che

$$(12), (23), (13), (123), (132) \notin Z(S_3).$$

Quindi $Z(S_3) = \{1\}$. Ragionando in maniera analoga per S_4, si prova che $Z(S_4) = \{1\}$.

5.40 (b) Si pensi al gruppo S_3.

5.41 Per il teorema di Lagrange si ha che

$$[G : H]|H| = |G| = [G : N]|N| = [G : N]([N : H]|H|),$$

da cui si deduce l'asserto cancellando $|H|$.

5.42 Poniamo $N = \langle g, H\rangle$ e osserviamo che $H < N$. Per l'esercizio 5.41 si ha $[G : H] = [G : N][N : H]$. Ora $[N : H] > 1$ per $H < N$, mentre $[G : H] = p$ per ipotesi. Quindi $[G : N] = 1$ e $N = \langle g, H\rangle = G$. Inoltre per ipotesi

$$g^2H = g(gH) = g(Hg) = (gH)g = (Hg)g = Hg^2,$$

da cui per induzione segue che $g^iH = Hg^i$ per ogni $i \in \mathbb{N}$. Dunque H è normale in $\langle g, H\rangle = G$.

5.45 Osserviamo che se $A = (a_{ij}) \in \mathrm{O}_n(K) \cap \mathrm{T}_n^-(K)$, allora $A^{-1} = (b_{ij}) \in \mathrm{T}_n^-(K)$, perché $\mathrm{T}_n^-(K)$ è un sottogruppo. Inoltre dal fatto che $A \in \mathrm{O}_n(K)$ segue che $A^{-1} = A^t$, cioè A è una matrice diagonale.

5.46 Ricordiamo che $\mathrm{O}_2(K) = \{A \in GL_2(K) : A^{-1} = A^t\}$. Si consideri la matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Allora $A \in GL_2(K)$ poiché $\det(A) = -1$. Inoltre $A^2 = I_2$, quindi

$$A^{-1} = A = A^t$$

e dunque $A \in \mathrm{O}_2(K)$. Data la matrice

$$H = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(K),$$

si verifica facilmente che

$$H^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

e quindi

$$B := H^{-1}AH = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Poiché $B^2 = I_2$ e $B \neq B^t$, possiamo concludere che $B \notin \mathrm{O}_2(K)$ e quindi $\mathrm{O}_2(K)$ non è normale in $GL_2(K)$.

5.47 (c) Data $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ considerare i casi $a \neq 0$ e $a = 0$.

5.56 Osserviamo che $xy = (yx)^{x^{-1}}$ e che se due elementi sono coniugati hanno lo stesso ordine.

13.6 Esercizi del capitolo 6

6.1 Siano $x, y \in H$. Allora

$$x = \frac{m}{p_1 p_2 \cdots p_s} \quad \text{ed} \quad y = \frac{n}{q_1 q_2 \cdots q_r}$$

ove $m, n \in \mathbb{Z}$ e p_i, q_j sono numeri primi per $i = 1, \ldots, s$, $j = 1, \ldots, r$ con $(p_i, p_j) = 1 = (q_i, q_j)$ se $i \neq j$. Siano $P := \{p_1, p_2, \ldots, p_s\}$ e $Q := \{q_1, q_2, \ldots, q_r\}$ e consideriamo i due casi seguenti:

- se $P \cap Q = \emptyset$, allora $p_i \neq q_j$ per ogni i, j e
$$x - y = \frac{(q_1 q_2 \ldots q_r)m - (p_1 p_2 \ldots p_s)n}{p_1 p_2 \ldots p_s q_1 q_2 \ldots q_r} \in H$$
per definizione di H.
- se $P \cap Q \neq \emptyset$ e $|P \cap Q| = k \geq 1$, con $k \leq \min\{r, s\}$, a meno di rinumerare i primi che compaiono nei denominatori di x e y possiamo supporre che $p_i = q_i$ per ogni $i = 1, \ldots, k$. Allora
$$x - y = \frac{(q_{k+1} q_{k+2} \cdots q_r)m - (p_{k+1} p_{k+2} \cdots p_s)n}{p_1 p_2 \cdots p_s q_{k+1} q_{k+2} \cdots q_r} \in H.$$
Per il lemma 5.29 possiamo concludere che $H \leq (\mathbb{Q}, +)$.

Dato l'elemento $\frac{5}{36} + H$ del gruppo quoziente $\mathbb{Q}/H$, osserviamo che $36 = (2 \cdot 3)^2$ e quindi

$$6\left(\frac{5}{36} + H\right) \in H.$$

Poiché

$$2\left(\frac{5}{36} + H\right) = \frac{5}{2 \cdot 3^2} + H \notin H \quad \text{e} \quad 3\left(\frac{5}{36} + H\right) = \frac{5}{2^2 \cdot 3} + H \notin H,$$

l'ordine di $\frac{5}{36} + H$ è 6.

6.5 Ricordiamo che date due matrici $A, B \in GL_2(\mathbb{R})$, $(AB)^t = B^t A^t$. Quindi l'applicazione $\tau : GL_2(\mathbb{R}) \to GL_2(\mathbb{R})$ definita da $A \mapsto A^t$ è un omomorfismo se e solo

$$B^t A^t = (AB)^t = \tau(AB) = \tau(A)\tau(B) = A^t B^t$$

per ogni coppia di matrici $A, B \in GL_2(\mathbb{R})$. Scelte $A = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$ e $B = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix}$, un semplice calcolo mostra che $\tau(AB) \neq \tau(A)\tau(B)$.

6.6 (a) Provare che l'applicazione $f : \mathbb{R} \to \mathbb{S}$ definita da $x \mapsto \cos(2\pi x) + i\,\text{sen}(2\pi x)$ è un omomorfismo suriettivo con $\ker f = \mathbb{Z}$. Per il teorema 6.12, $(\mathbb{R}/\mathbb{Z}, +) \cong (\mathbb{S}, \cdot)$.

(c) Provare che l'applicazione $\psi_n : \mathbb{Z} \to \mathbb{U}_n$ definita da

$$k \mapsto \cos\left(\frac{2\pi k}{n}\right) + i \operatorname{sen}\left(\frac{2\pi k}{n}\right)$$

è un omomorfismo suriettivo con $\ker \psi_n = n\mathbb{Z}$. Per il teorema 6.12,

$$(\mathbb{Z}/n\mathbb{Z}, +) \cong (\mathbb{U}_n, \cdot).$$

6.7 Confrontare gli ordini degli elementi.

6.8 Per dimostrare che f e g coincidono, verifichiamo che esse coincidono su ogni elemento $y \in G$ del dominio. Poiché $G = \langle X \rangle$, un generico elemento $y \in G$ è della forma $y = x_1^{\alpha_1} \dots x_s^{\alpha_s}$ ove $s \in \mathbb{N}_+$, $\alpha_i \in \mathbb{Z}$, $x_i \in X$ per $i = 1, \dots, s$. Allora l'ipotesi $f(x) = g(x)$ per ogni $x \in X$ implica che

$$f(y) = f(x_1)^{\alpha_1} \dots f(x_s)^{\alpha_s} = g(x_1)^{\alpha_1} \dots g(x_s)^{\alpha_s} = g(y).$$

6.9 Consideriamo i casi (a) e (b) in cui F è finito e sia $F = \{(x_1, y_1), \dots, (x_n, y_n)\}$. Se F è vuoto non abbiamo niente da dimostrare. Supponiamo che l'insieme F sia non vuoto e poniamo $Y = \{y_1, \dots, y_n\}$.

Per verificare che f è un omomorfismo è sufficiente che valga $f(xy) = f(x)f(y)$ per ogni $(x, y) \in F$. Lo faremo per la coppia (x_1, y_1), per le altre si ragiona analogamente.

Sia $Y_1 = Y \cup Y^{-1} \cup y_1 Y^{-1}$. Poiché $|Y_1| \leq 3 \cdot |Y| = 3 \cdot |F|$, sicuramente $Y_1 \neq G$ nei casi (a) e (b). Sia $y \in G \setminus Y_1$.

Poiché $y \notin Y$, si ha $(1, y) \notin F$, pertanto vale $f(y) = f(1 \cdot y) = f(1)f(y)$ da cui $f(1) = 1$.

Ora possiamo verificare che $f(x_1 y_1) = f(x_1)f(y_1)$. Infatti

$$\begin{aligned} f(x_1 y_1) &= f(x_1 y_1 y^{-1} y) = f(x_1 y_1 y^{-1}) f(y) = f(x_1) f(y_1 y^{-1}) f(y) = \\ &= f(x_1) f(y_1) f(y^{-1}) f(y) = f(x_1) f(y_1) f(y^{-1} y) = \\ &= f(x_1) f(y_1) f(1) = f(x_1) f(y_1). \end{aligned}$$

La prima e la sesta uguaglianza sono ovvie e la settima vale perché $f(1) = 1$. La seconda e la quinta uguaglianza valgono perché $y \neq y_i$, la terza perché $y_1 y^{-1} \neq y_i$, la quarta perché $y^{-1} \neq y_i$, per ogni $i = 1, \dots, n$.

Nel caso (c) si ragiona analogamente, con $Y = p_2(F)$ la proiezione di

$$F \subseteq G \times G$$

sulla seconda componente G e $Y_1 = Y \cup Y^{-1} \cup y_1 Y^{-1}$. Di nuovo $|Y_1| < |G|$; se F è infinito, usiamo il fatto che $|Y_1| \leq |F| < |G|$, altrimenti $|Y_1| \leq 3 \cdot |F| < |G|$.

6.14 Mediante gli isomorfismi $H \cong H \times \{1\}$ e $K \cong \{1\} \times K$ possiamo identificare i sottogruppi normali $H \times \{1\}$ e $A \cap (\{1\} \times K)$ di A rispettivamente con H e $A \cap K$. Poiché $H \cap (A \cap K) \subseteq H \cap K = \{1\}$, il sottogruppo $H(A \cap K)$ di A è isomorfo al prodotto diretto $H \times A \cap K$. Per concludere resta da provare che

$H(A \cap K) = A$. Scelto un elemento $a \in A$, esistono $h \in H$ e $k \in K$ tali che $a = (h, k) = (h, 1_K)(1_H, k)$. Conseguentemente

$$(1_H, k) = (h, 1_K)^{-1}(h, k) \in (\{1\} \times K) \cap A = A \cap K$$

e quindi $A \leq H(A \cap K)$.

6.15 (b) Supponiamo per assurdo che $N \cap H = \{1\}$ e $N \cap K = \{1\}$. Allora per il lemma 6.34, si ha che che gli elementi di N commutano con tutti gli elementi di H e con tutti gli elementi K, cioè con tutti gli elementi di G, da cui $N \leq Z(G)$ in contraddizione con l'ipotesi.

(c) Sia N un sottogruppo normale non banale di G. Per (a), il centro di G è $\{1\}$ e quindi per (b), si ha per esempio che $N \cap H$ è un sottogruppo normale non identico di H. Allora $N \cap H = H$. Ora $N = H(N \cap K)$ per l'esercizio 6.14. Il sottogruppo $N \cap K$ è un sottogruppo normale di K, quindi coincide con $\{1\}$ oppure K. Il secondo caso non è possibile perché altrimenti $N = G$. Quindi $N \cap K = \{1\}$ e $N = H$. Se invece $H \cap N = \{1\}$, allora il punto (b) permette di ragionare con K al posto di H.

6.16 (a) Si verifica facilmente che

$$1_G = (0, 0, 0) \quad \text{e} \quad (a, b, c)^{-1} = (-a, -b + ac, -c).$$

(b) Dati $a, b, c, a', b', c' \in \mathbb{Z}$ vale

$$f((a, b, c) \cdot (a', b', c')) = f((a + a', b + b' + ac', c + c')) = (a + a', c + c') =$$
$$= (a, c) + (a, c') = f((a, b, c)) \cdot f((a', b', c')),$$

dunque f è un omomorfismo e

$$\ker(f) = \{(a, b, c) \in G : f((a, b, c)) = (0, 0)\} = \{(a, b, c) \in G : a = 0,\ c = 0\})$$
$$= \{(0, b, 0) : b \in \mathbb{Z}\}.$$

(c) L'inclusione $\ker f \subseteq Z(G)$ è banale. Viceversa, sia $(x, y, z) \in Z(G)$. Allora, scelto $b \in \mathbb{Z} \setminus \{0\}$, l'uguaglianza

$$(x + 1, y + b + 0, z) = (x, y, z)(1, b, 0) =$$
$$= (1, b, 0)(x, y, z) = (1 + x, y + b + z, z)$$

implica che $z = 0$. Analogamente, l'uguaglianza

$$(x, b + y + x, 1) = (x, y, 0)(0, b, 1) = (0, b, 1)(x, y, 0) = (x, b + y, 1)$$

implica che $x = 0$ e quindi $Z(G) \subseteq \ker f$.

6.18 Per (b) considerare l'applicazione $f : K \times H \to G$ definita da $f(k, h) = k + h$. Si verifichi che f è un omomorfismo la cui immagine è $K + H$. Per (c) notare che l'ordine del sottogruppo $K \cap H$ divide sia $|K|$ che $|H|$. Pertanto $|K \cap H| = 1$ e quindi $K + H \cong K \times H$.

6.19 Sia x un elemento non nullo di G. Poiché G non è ciclico, $H = \langle x \rangle$ ha ordine 3. Sia $y \in G \setminus H$. Allora $K = \langle y \rangle$ ha tre elementi e $K \not\subseteq H$. Quindi $H \cap K = \{1\}$ e HK contiene propriamente K. Poiché $|HK|$ divide $9 = |G|$, concludiamo che $HK = G$. Ora si applichi il corollario 6.37.

6.20 Sia $z = (x, y)$ un elemento di G. Se $x \neq 0$ e $y \neq 0$, allora $o(x) = p$, $o(y) = q$ e quindi $o(z) = pq$ per la proposizione 6.40. Pertanto il sottogruppo ciclico $\langle z \rangle$ coincide con tutto G. Se invece $z = (x, 0)$, con $x \neq 0$, il sottogruppo ciclico $\langle z \rangle$ coincide con $\mathbb{Z}_p \times \{0\}$. Se $z = (0, y)$, con $y \neq 0$, il sottogruppo ciclico $\langle z \rangle$ coincide con $\{0\} \times \mathbb{Z}_q$. Abbiamo così descritto tutti i possibili sottogruppi di G. Questo dimostra che G ha quattro sottogruppi.

6.21 Ogni sottogruppo proprio di $\mathbb{Z}_p \times \mathbb{Z}_p$ è di ordine p e quindi ciclico. Siano H e K due sottogruppi propri distinti. Allora $H \cap K = \{0\}$, quindi ogni elemento $x \neq 0$ di $\mathbb{Z}_p \times \mathbb{Z}_p$ è contenuto in un solo sottogruppo proprio di $\mathbb{Z}_p \times \mathbb{Z}_p$. Poiché $\mathbb{Z}_p \times \mathbb{Z}_p$ ha $p^2 - 1$ elementi non nulli e poiché ogni sottogruppo proprio contiene $p - 1$ elementi non nulli, deduciamo che il numero dei sottogruppi propri di $\mathbb{Z}_p \times \mathbb{Z}_p$ è $p+1 = \frac{p^2-1}{p-1}$.

6.22 Siano G e H due sottogruppi di S_3 tali che $S_3 \cong G \times H$. Allora $|G|$ e $|H|$ dividono 6, quindi possono essere solo 2 e 3. Di conseguenza G e H sono ciclici e quindi abeliani. Allora S_3 deve essere abeliano, assurdo.

6.23 (a) Siano $g \in G$ e $k = o(g)$. Allora

$$1_H = f(1_G) = f(g^k) = f(g)^k$$

e quindi $o(f(g))$ divide k per il lemma 5.5 (a).

(b) Se $g \in \ker f$, allora $f(g) = 1_H$ e dunque $o(f(g)) = 1$. L'ipotesi

$$o(f(g)) = o(g) \quad \text{per ogni } g \in G$$

implica ora che $g = 1_G$.

(c) Se l'omomorfismo f è suriettivo, allora $G/\ker f \cong H$ per il primo teorema di isomorfismo. Poiché

$$|H| = |G/\ker f| = [G : \ker f]$$

e, per il teorema di Lagrange, $|G| = [G : \ker f]|\ker f|$, possiamo concludere che $|H|$ divide $|G|$.

(d) Se l'omomorfismo f è iniettivo, allora $G \cong f(G)$ e quindi $|G| = |f(G)|$. Essendo H finito, il teorema di Lagrange garantisce che $|f(G)|$ divide $|H|$ e quindi la tesi.

6.24 Essendo G abeliano, $f(G)$ e $\ker f$ sono sottogruppi normali di G. Proviamo che $f(G) \cap \ker f = \{1\}$. Infatti, se $x \in f(G) \cap \ker f$, $f(x) = 1$ e $x = f(g)$ per un opportuno elemento $g \in G$. Poiché $f^2 = f$, otteniamo che

$$1 = f(x) = f(f(g)) = f(g) = x.$$

Per concludere è sufficiente verificare che $G = f(G) \ker f$. L'inclusione

$$f(G) \ker f \subseteq G$$

è ovvia. Per dimostrare l'altra inclusione, consideriamo un generico elemento $g \in G$. Poiché $f(f(g)) = f(g)$, si ha che $gf(g)^{-1} \in \ker f$ e quindi $g \in f(G) \ker f$.

6.27 (b) Un elemento $x+iy \in G$ appartiene al nucleo di f se e solo se $f(x+iy) = 0$ se e solo se $x + y = 0$ se e solo se $y = -x$ se e solo se $x + iy \in \{x - ix : x \in \mathbb{Z}\}$ se e solo se $x + iy \in \langle 1 - i \rangle$.

6.31 Osserviamo che per ogni $i = 1, \ldots, r$, $H_i \trianglelefteq G$ in quanto prodotto di sottogruppi normali, per il lemma 5.69. Facciamo induzione su r. Il caso $r = 2$ è il teorema 6.35. Supponiamo $r \geq 3$. Allora H_r e i suoi sottogruppi $N_1, \ldots, N_{r-1}$ soddisfano le ipotesi della proposizione. Se poniamo $K_i = H_r \cap H_i$ per ogni $i = 1, \ldots, r-1$, si ha infatti $N_i \cap K_i \leq N_i \cap H_i = \{1\}$ per ogni $i = 1, \ldots, r-1$ e $H_r = N_1 \ldots N_{r-1}$. Applicando l'ipotesi induttiva ad H_r si ottiene $H_r \cong N_1 \times \ldots \times N_{r-1}$. Inoltre G, H_r ed N_r soddisfano le ipotesi del teorema 6.35 e si conclude:

$$G \cong H_r \times N_r \cong N_1 \times \ldots \times N_r.$$

6.36 Sia $\mathcal{H}$ la famiglia dei sottogruppi H di $\mathbb{R}$ tali che $\mathbb{Q} \cap H = \{0\}$. Essendo $\{0\} \in \mathcal{H}$, la famiglia $\mathcal{H}$ non è vuota. La rendiamo un insieme ordinato rispetto all'inclusione $\subseteq$. Non è difficile verificare che l'insieme ordinato $(\mathcal{H}, \subseteq)$ risulta induttivo. Pertanto esiste un elemento massimale H di $\mathcal{H}$ per il lemma di Zorn. Dalla scelta di H segue $\mathbb{Q} \cap H = \{0\}$, quindi basta verificare che $\mathbb{R} = \mathbb{Q} + H$ per concludere che $\mathbb{R} \cong \mathbb{Q} \times H$. Sia H_1 l'insieme di tutti gli $x \in \mathbb{R}$ tali che $nx \in H$ per qualche intero $n > 0$. Allora H_1 è un sottogruppo di $\mathbb{R}$ contenente H. Non è difficile verificare che $\mathbb{Q} \cap H_1 = \{0\}$. Per la scelta di H concludiamo che $H_1 = H$. Sia ora $x \in \mathbb{R}$ con $x \notin H$. Allora il sottogruppo $H_2 = \langle x, H \rangle$ contiene propriamente H e quindi esiste un elemento non nullo $q \in \mathbb{Q} \cap H_2$. Sia $q = kx + h$, con $k \in \mathbb{Z}$ e $h \in H$. Allora $k \neq 0$, poiché altrimenti $q = h \in \mathbb{Q} \cap H = \{0\}$, assurdo. Sia h_1 l'unico numero reale con $kh_1 = h$. Allora $h_1 \in H_1 = H$ e $x = (1/k)q - h_1 \in \mathbb{Q} + H$.

6.40 Se si considera il sottogruppo ciclico $C = \langle -1 \rangle = \{1, -1\}$ di $(\mathbb{R}^*, \cdot)$ si ha

$$\mathbb{R}_+ \cap C = \{1\} \quad \text{e} \quad \mathbb{R}_+ \cdot C = \mathbb{R}^*,$$

dove $(\mathbb{R}_+, \cdot)$ è il sottogruppo di $(\mathbb{R}^*, \cdot)$ formato da tutti i numeri reali positivi. Quindi $(\mathbb{R}^*, \cdot) \cong \mathbb{R}_+ \times C$ per il teorema 6.35. Poiché il sottogruppo $(\mathbb{R}_+, \cdot)$ di $(\mathbb{R}^*, \cdot)$ è isomorfo a $(\mathbb{R}, +)$, e $C \cong (\mathbb{Z}_2, +)$, abbiamo $(\mathbb{R}^*, \cdot) \cong \mathbb{Z}_2 \times (\mathbb{R}, +)$.

6.41 Gli elementi di periodo n sono esattamente le classi laterali $\overline{k/n}$, dove $1 \leq k < n$ e k è coprimo con n. Pertanto per ogni numero naturale $n > 1$ il gruppo $\mathbb{R}/\mathbb{Z}$ ha precisamente $\varphi(n)$ elementi di periodo n.

13.7 Esercizi del capitolo 7

7.4 Applicare il teorema di Frobenius-Stickelberger.

7.9 Si usino gli esercizi 7.7 e 7.8.

7.10 Poiché G è abeliano, $\langle x, y\rangle = \langle x\rangle + \langle y\rangle$. Quindi per l'esercizio 6.18, $|G|$ divide $|\langle x\rangle||\langle y\rangle|$, da cui segue che p divide $o(x)o(y)$. Ora dal fatto che p non divide $o(x)$ segue che p divide $o(y)$.

7.11 Il numero degli elementi di $\mathbb{Z}_{p^k}^m$ di ordine p^s è 0 se $s > k$, perciò assumiamo $s \leq k$. Allora $x = (x_1, \ldots, x_m) \in G$ ha $o(x) \leq p^s$ se e solo se $p^s x_i = 0$ per ogni $i = 1, \ldots, m$. Quindi ci sono p^{ms} elementi x con questa proprietà. Per lo stesso motivo, ci sono $p^{m(s-1)}$ elementi x con $o(x) \leq p^{s-1}$, cioè $o(x) < p^s$. Allora il numero degli elementi x con periodo $o(x) = p^s$ è $p^{ms} - p^{m(s-1)}$

7.12 Se $r > s$, questo numero è 0 perciò assumiamo $r \leq s$. Allora $x \in G$ ha $o(x) \leq p^r$ se e solo se x appartiene al sottogruppo

$$G_1 = \mathbb{Z}_p^{m_1} \times \mathbb{Z}_{p^2}^{m_2} \times \ldots \times \mathbb{Z}_{p^r}^{m_r} \times \mathbb{Z}_{p^r}^{m_{r+1}} \times \mathbb{Z}_{p^r}^{m_{r+2}} \times \ldots \times \mathbb{Z}_{p^r}^{m_s}$$

di G. Perciò ci sono $|G_1| = p^{\sum_{i=1}^r im_i + r\sum_{i=r+1}^s m_i}$ elementi di ordine al più p^r in G. Ora si prosegue come nello svolgimento dell'esercizio 7.11.

7.13 Dimostrare che si può assumere senza ledere la generalità che esiste un numero primo p, tale che G ed H hanno solamente elementi di periodo potenza di p. Per il teorema di Frobenius-Stickelberger possiamo scrivere

$$G = \mathbb{Z}_p^{m_1} \times \mathbb{Z}_{p^2}^{m_2} \times \ldots \times \mathbb{Z}_{p^s}^{m_s}$$

e

$$H = \mathbb{Z}_p^{n_1} \times \mathbb{Z}_{p^2}^{n_2} \times \ldots \times \mathbb{Z}_{p^t}^{n_t}.$$

Supponiamo $s \geq t$. Paragonando il numero degli elementi di ordine p^s in G e in H concludiamo che $s = t$. Procediamo ora per induzione su s. L'asserto è ovvio per $s = 1$. Supponiamo $s > 1$ e l'asserto sia vero per ogni coppia di gruppi G e H con $p^{s-1}G = p^{s-1}H = 0$. Consideriamo ora i sottogruppi

$$G_1 = \mathbb{Z}_p^{m_1} \times \mathbb{Z}_{p^2}^{m_2} \times \ldots \times \mathbb{Z}_{p^{s-1}}^{m_{s-1}} \times \mathbb{Z}_{p^{s-1}}^{m_s}$$

e

$$H_1 = \mathbb{Z}_p^{n_1} \times \mathbb{Z}_{p^2}^{n_2} \times \ldots \times \mathbb{Z}_{p^{s-1}}^{n_{s-1}} \times \mathbb{Z}_{p^{s-1}}^{n_s}$$

di G e H rispettivamente. Chiaramente G_1 (rispettivamente H_1) consiste di tutti gli elementi di ordine al più p^{s-1} in G (in H, rispettivamente). Pertanto la coppia di gruppi G_1 e H_1 soddisfa l'ipotesi di partenza di avere un numero uguale di elementi di periodo k per ogni k, avendo in più la proprietà $p^{s-1}G_1 = p^{s-1}H_1 = 0$. Scrivendo

$$\mathbb{Z}_{p^{s-1}}^{m_{s-1}} \times \mathbb{Z}_{p^{s-1}}^{m_s} = \mathbb{Z}_{p^{s-1}}^{m_{s-1}+m_s}$$

e

$$\mathbb{Z}_{p^{s-1}}^{n_{s-1}} \times \mathbb{Z}_{p^{s-1}}^{n_s} = \mathbb{Z}_{p^{s-1}}^{n_{s-1}+n_s}$$

e applicando l'ipotesi induttiva concludiamo che $G_1 \cong H_1$ e

$$m_1 = n_1, m_2 = n_2, \dots, m_{s-2} = n_{s-2} \text{ e } m_{s-1} + m_s = n_{s-1} + n_s. \qquad (6)$$

Poiché G (rispettivamente H), ha $|G| - |G_1|$ (rispettivamente $|H| - |H_1|$) elementi di ordine p^s, concludiamo che $|G| = |H|$, essendo l'uguaglianza $|G_1| = |H_1|$ già verificata. Ora calcolando $|G| = |H|$ troviamo

$$p^{\sum_{i=1}^{s-2} im_i + (s-1)m_{s-1} + sm_s} = p^{\sum_{i=1}^{s-2} in_i + (s-1)n_{s-1} + sn_s},$$

e quindi

$$\sum_{i=1}^{s-2} im_i + (s-1)m_{s-1} + sm_s = \sum_{i=1}^{s-2} in_i + (s-1)n_{s-1} + sn_s. \qquad (7)$$

Da (6) si ha

$$\sum_{i=1}^{s-2} im_i = \sum_{i=1}^{s-2} in_i$$

e

$$(s-1)m_{s-1} + (s-1)m_s = (s-1)n_{s-1} + (s-1)n_s.$$

Pertanto (7) implica $m_s = n_s$ e di conseguenza anche $m_{s-1} = n_{s-1}$ sempre per (6).

7.14 (c) Supponiamo $x^2 = 1_A$ per ogni $x \in A$. Allora $x = x^{-1}$ per ogni $x \in A$ e quindi $\tau(x) = x$ per ogni $x \in A$, cioè $\tau = id_A$. Se esiste $x \in A \setminus \{1_A\}$ tale che $x^2 \neq 1_A$, si ha $x \neq x^{-1}$ e quindi $\tau(x) \neq x$. In particolare, $\tau \neq id_A$. D'altra parte, la definizione di τ implica che $\tau^2(a) = \tau(\tau(a)) = a$ per ogni $a \in A$ e quindi $\tau^2 = id_A$. Ciò prova che $o(\tau) = 2$ in $\mathrm{Aut}(A)$.

7.15 (a) Basta prendere $r = f(1)$ e notare che $f(n) = nf(1) = nr$. Inoltre, se $m \neq 0$ e $x = 1/m$, allora

$$r = f(1) = f(mx) = mf(x) \in \mathbb{Q}.$$

Ne deduciamo che $f(x) = \left(\frac{1}{m}\right) r$. Se $x = \frac{n}{m}$, $m \neq 0$, allora

$$f(x) = nf\left(\frac{1}{m}\right) = n\left(\left(\frac{1}{m}\right) r\right) = \left(\frac{n}{m}\right) r.$$

(c) Notare che ogni automorfismo del gruppo $(\mathbb{Q} \times \mathbb{Q}, +)$ è anche un'applicazione lineare invertibile dello spazio vettoriale $\mathbb{Q} \times \mathbb{Q}$ sopra il campo $\mathbb{Q}$. Si ragiona analogamente per (d).

7.16 Caso $n = 9$: osserviamo che $|G| = \varphi(9) = 6$. Inoltre $a = [2]_9 \in G$ soddisfa $a^2 \neq 1$ e $a^3 \neq 1$, mentre $a^6 = 1$. Quindi $o(a) = 6$. Pertanto $G = \langle a \rangle$ è ciclico e $G \cong \mathbb{Z}_6$.

Caso $n = 20$: poiché $\varphi(20) = 8$, G ha otto elementi:

$$G = \{[1]_{20}, [3]_{20}, [7]_{20}, [9]_{20}, [11]_{20}, [13]_{20}, [17]_{20}, [19]_{20}\}.$$

Si vede facilmente che

$$[9]_{20}^2 = [11]_{20}^2 = [19]_{20}^2 = [1]_{20}.$$

Pertanto

$$o([9]_{20}) = o([11]_{20}) = o([19]_{20}) = 2$$

e $K = \langle [11]_{20} \rangle$ ha due elementi. Inoltre $[3]_{20}^4 = [1]_{20}$, ma $[3]_{20}^2 \neq [1]_{20}$. Quindi $o([3]_{20}) = 4$ e

$$H = \langle [3]_{20} \rangle = \{[1]_{20}, [3]_{20}, [9]_{20}, [7]_{20}\}$$

non contiene $[11]_{20}$, da cui segue $K \cap H = \{[1]_{20}\}$. Il sottogruppo HK di G generato da $[11]_{20}$ e $[3]_{20}$ contiene propriamente H, quindi $d = |HK| > 4$ e d divide $8 = |G|$. Dunque $d = 8$ essendo d un multiplo di 4. Allora $HK = G$. Ora il teorema 6.35 implica $G \cong H \times K \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, essendo $H \cong \mathbb{Z}_4$ e $K \cong \mathbb{Z}_2$.

Caso $n = 21$: si noti che $2^6 \equiv_{21} 1$, mentre $2^3 \not\equiv_{21} 1$ e $2^2 \not\equiv_{21} 1$. Quindi $[2]_{21}$ ha periodo 6 nel gruppo $U(\mathbb{Z}_{21})$ degli elementi invertibili di $\mathbb{Z}_{21}$. Poiché $\langle [2]_{21} \rangle \cap K = \{1\}$ per il sottogruppo ciclico $K = \langle [20]_{21} \rangle$ e $\langle [2]_{21} \rangle \cong \mathbb{Z}_6$, concludiamo che

$$U(\mathbb{Z}_{21}) \cong \mathbb{Z}_6 \times \mathbb{Z}_2.$$

Infine $\mathrm{Aut}(\mathbb{Z}_{21}) \cong U(\mathbb{Z}_{21})$.

Caso $n = 24$: $\mathrm{Aut}(\mathbb{Z}_{24}) \cong \mathrm{Aut}(\mathbb{Z}_3) \times \mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
Caso $n = 60$: $\mathrm{Aut}(\mathbb{Z}_{60}) \cong \mathrm{Aut}(\mathbb{Z}_4) \times \mathrm{Aut}(\mathbb{Z}_3) \times \mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$.
Caso $n = 72$: $\mathrm{Aut}(\mathbb{Z}_{72}) \cong \mathrm{Aut}(\mathbb{Z}_8) \times \mathrm{Aut}(\mathbb{Z}_9) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$.

7.18 Siano $u, v \in \mathbb{Z}$ tali che $1 = um + vn$ e sia x un arbitrario elemento di G. Allora $x = (x^m)^u (x^n)^v = (x^v)^n$ poiché $o(x)$ divide $m = |G|$. Di conseguenza $f(x) = f((x^v)^n) = (f(x^v))^n = 1$ poiché $o(f(x^v))$ divide $n = |H|$.

7.19 Sia $f(x, y) = (t_1(x, y), t_2(x, y))$ la coppia corrispondente alla coppia (x, y) tramite l'omomorfismo f. Consideriamo gli omomorfismi

$$t_1 = p_1 \circ f \quad \text{e} \quad t_2 = p_2 \circ f,$$

dove p_1, p_2 sono le proiezioni del prodotto $\mathbb{Z}_m \times \mathbb{Z}_n$. Si ha

$$t_1(x, y) = p_1(f(x, y)) \quad \text{per } x \in \mathbb{Z}_m, y \in \mathbb{Z}_n.$$

La restrizione di t_1 al sottogruppo $\{0\} \times \mathbb{Z}_n$ è banale per l'esercizio 7.18. Quindi t_1 dipende solamente da x, cioè

$$t_1(x, y) = t_1(x, 0)$$

per ogni $y \in \mathbb{Z}_n$. Denoteremo con f_1 l'applicazione $x \mapsto t_1(x, 0)$ da $\mathbb{Z}_m$ a $\mathbb{Z}_m$ c ricavata. Analogamente si vede che t_2 dipende solamente da y e la si può consid e come un omomorfismo $f_2 : \mathbb{Z}_n \to \mathbb{Z}_n$. Ora resta da notare che

$$f(x,y) = (t_1(x,y), t_2(x,y)) = (t_1(x,0), t_2(0,y)) = (f_1(x), f_2(y))$$

per ogni coppia $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$.

7.20 Sia $\varphi : \mathrm{Aut}(G) \to \mathrm{Aut}(\mathbb{Z}_m) \times \mathrm{Aut}(\mathbb{Z}_n)$ l'applicazione che associa ad ogni automorfismo f di G la coppia di automorfismi (f_1, f_2) come definiti nel precedente esercizio 7.19. Si dimostri che φ è un isomorfismo.

7.21 Ragionare come negli esercizi 7.19 e 7.20.

7.22 Notare che ogni automorfismo del gruppo $(\mathbb{Z}_p \times \mathbb{Z}_p, +)$ è anche un'applicazione lineare invertibile dello spazio vettoriale $\mathbb{Z}_p \times \mathbb{Z}_p$ sul campo $\mathbb{F}_p$.

7.23 Per il lemma di Cauchy esistono sottogruppi H e K di G con

$$|H| = 5 \qquad \text{e} \quad |K| = 3.$$

Per l'esercizio 8.32a), H è normale, essendo $[G : H] = 3$. Sia a un generatore di K, quindi $o(a) = 3$. Allora il coniugio φ_a di G soddisfa $(\varphi_a)^3 = id_G$. Essendo H un sottogruppo normale di G, abbiamo $\varphi_a(H) = H$. In particolare φ_a induce un automorfismo f di $H \cong \mathbb{Z}_5$. Poiché il gruppo $\mathrm{Aut}(\mathbb{Z}_5)$ non ha elementi di ordine 3, l'automorfismo f deve essere identico. Quindi a commuta con tutti gli elementi di H. Ovviamente lo stesso vale anche per a^2. Poiché $G = \langle a, H \rangle$, il gruppo G risulta abeliano. Per il corollario 6.37 abbiamo

$$G \cong K \times H \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}.$$

7.24 Per il lemma di Cauchy esistono sottogruppi H e K di G con $|H| = p$ e $|K| = q$. Per il corollario 6.37 abbiamo

$$G \cong K \times H \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

7.25 Se $\mathbb{Z}_2 = \langle x \rangle$ e $\mathbb{Z}_4 = \langle y \rangle$, allora ogni $f \in G = \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4)$ è determinato dai valori $f(x) = (x, 2sy)$ e $f(y) = (kx, ey)$, dove $s, k = 0, 1$ ed $e = \pm 1$. Pertanto ci sono 8 automorfismi di $\mathbb{Z}_2 \times \mathbb{Z}_4$. Si provi che G non è abeliano, possiede un elemento di ordine 4 e possiede più di un elemento di periodo 2, quindi G non può essere il gruppo dei quaternioni Q_8. Si dimostra infine che $G \cong D_8$.

7.27 Sia $H \leq \mathbb{Q}/\mathbb{Z}$ e sia $\pi : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ l'omomorfismo canonico. Allora $\pi^{-1}(H) = H + \mathbb{Z}$ è un sottogruppo finitamente generato di $\mathbb{Q}$, in quanto somma di sottogruppi finitamente generati. Allora per la proposizione 7.17, $H + \mathbb{Z}$ è ciclico e così la sua immagine $\pi(H + \mathbb{Z}) = H$ è ciclico.

7.28 Ragionando per assurdo supponiamo che $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ sia un isomorfismo. Il sottogruppo $H = \mathbb{Z} \times \mathbb{Z}$ di $\mathbb{Q} \times \mathbb{Q}$ non è ciclico, quindi nemmeno il sottogruppo $f(H) \cong H$ di $\mathbb{Q}$ è ciclico. D'altra parte, H è finitamente generato, quindi anche $f(H)$ è finitamente generato. Per la proposizione 7.17, $f(H)$ deve essere ciclico, assurdo.

Per dimostrare che $\mathbb{R} \times \mathbb{R}$ è isomorfo a $\mathbb{R}$, bisogna provare che $\mathbb{R}$ come spazio vettoriale sopra $\mathbb{Q}$ ha dimensione infinita, cioè ha una base infinita B. Trovando una partizione $B = B_1 \cup B_2$ di B con $|B_1| = |B_2| = |B|$ si dimostra che i sottospazi V_1 e V_2 dello spazio $\mathbb{R}$ generati da B_1 e B_2 rispettivamente, sono isomorfi entrambi a $\mathbb{R}$ e quindi $\mathbb{R} \cong V_1 \times V_2 \cong \mathbb{R} \times \mathbb{R}$.

7.30 Se esiste un divisore proprio n di m tale che $nx = 0$ per ogni $x \in G$ allora G non può essere ciclico, in quanto ogni elemento ha ordine minore di m. Supponiamo ora che G non sia ciclico e cerchiamo di trovare un divisore proprio n di m tale che $nx = 0$ per ogni $x \in G$. Sia $m = p_1^{k_1} \dots p_s^{k_s}$, con numeri primi distinti $p_1, \dots, p_s$. Ragioniamo per induzione su s. Sia $s = 1$. Non essendo G ciclico, ogni elemento $x \in G$ ha ordine minore di $m = p_1^{k_1}$. Ma $o(x)$ è sempre un divisore di m, quindi $o(x) = p^l$ per qualche $l < k_1$. Pertanto $p^{k_1 - 1}x = 0$ per ogni $x \in G$. Supponiamo ora $s > 1$ e supponiamo l'asserto vero per $s - 1$. Poniamo $m_1 = p_1^{k_1} \dots p_{s-1}^{k_{s-1}}$ e $m_2 = p_s^{k_s}$. Allora $(m_1, m_2) = 1$ e applicando la proposizione 7.13 a $G_1 = \{x \in G : m_1 x = 0\}$ e $G_2 = \{x \in G : m_2 x = 0\}$ si conclude che $|G_1| = m_1, |G_2| = m_2$ e $G \cong G_1 \times G_2$. Almeno uno dei gruppi G_1, G_2 non è ciclico per il teorema 6.42. Se questo è G_2, allora per la prima parte della dimostrazione, caso $s = 1$, esiste un divisore proprio d di m_2 tale che $dx = 0$ per ogni $x \in G_2$. Osserviamo che $m_1 d$ è un divisore proprio di m e $m_1 dy = 0$ per ogni $y \in G$. Se invece G_1 non è ciclico, per l'ipotesi induttiva esiste un divisore proprio d' di m_1 tale che $dz = 0$ per ogni $z \in G_1$. Chiaramente $d'm_2$ è un divisore proprio di m e $d'm_2 y = 0$ per ogni $y \in G$.

7.32 (a) $\mathbb{Z}_2 \times \mathbb{Z}_2$ ha tre sottogruppi propri non banali, ognuno di ordine 2.

(b) $\mathbb{Z}_2 \times \mathbb{Z}_3$ ha due sottogruppi propri non banali: $\mathbb{Z}_2 \times \{0\}$ e $\{0\} \times \mathbb{Z}_3$;

(c) $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ ha quattro sottogruppi propri non banali, ognuno di ordine 3. Infatti G ha 8 elementi non nulli, e i sottogruppi da essi generati sono 4, in quanto x e $-x$ generano lo stesso sottogruppo ciclico.

(f) $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ ha sei sottogruppi propri non banali: tre ciclici che non contengono alcun sottogruppo non banale

$$\mathbb{Z}_2 \times \{0\} \times \{0\}, \qquad \{0\} \times \mathbb{Z}_3 \times \{0\} \qquad \text{e} \qquad \{0\} \times \{0\} \times \mathbb{Z}_5;$$

e tre ciclici che non sono contenuti in alcun sottogruppo proprio:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \{0\}, \qquad \{0\} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \qquad \text{e} \qquad \mathbb{Z}_2 \times \{0\} \times \mathbb{Z}_5.$$

(g) Tutti i sottogruppi del gruppo $G = \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ sono della forma $A \times B \times C \times D$, dove $A \leq \mathbb{Z}_3$, $B \leq \mathbb{Z}_4$, $C \leq \mathbb{Z}_5$ e $D \leq \mathbb{Z}_7$. Quindi ci sono ventiquattro sottogruppi in totale.
G ha quattro sottogruppi ciclici che non contengono alcun sottogruppo non banale:

$$\mathbb{Z}_3 \times \{0\} \times \{0\} \times \{0\}, \qquad \{0\} \times \mathbb{Z}_2 \times \{0\} \times \{0\},$$

$$\{0\} \times \{0\} \times \mathbb{Z}_5 \times \{0\}, \qquad \{0\} \times \{0\} \times \{0\} \times \mathbb{Z}_7,$$

e quattro sottogruppi che non sono contenuti in alcun sottogruppo proprio:

$$\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \{0\}, \qquad \mathbb{Z}_3 \times \mathbb{Z}_4 \times \{0\} \times \mathbb{Z}_7,$$
$$\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7, \qquad \{0\} \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7.$$

e altri quattordici sottogruppi:

$$\mathbb{Z}_3 \times \mathbb{Z}_4 \times \{0\} \times \{0\}, \qquad \mathbb{Z}_3 \times \mathbb{Z}_2 \times \{0\} \times \{0\},$$
$$\mathbb{Z}_3 \times \{0\} \times \mathbb{Z}_5 \times \{0\}, \qquad \mathbb{Z}_3 \times \{0\} \times \{0\} \times \mathbb{Z}_7,$$
$$\mathbb{Z}_3 \times \{0\} \times \mathbb{Z}_5 \times \mathbb{Z}_7, \qquad \{0\} \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \{0\},$$
$$\{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \{0\}, \qquad \{0\} \times \{0\} \times \mathbb{Z}_5 \times \mathbb{Z}_7,$$
$$\{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7, \qquad \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \{0\},$$
$$\{0\} \times \mathbb{Z}_4 \times \{0\} \times \{0\}, \qquad \{0\} \times \mathbb{Z}_4 \times \{0\} \times \mathbb{Z}_7,$$
$$\{0\} \times \mathbb{Z}_2 \times \{0\} \times \mathbb{Z}_7, \qquad \mathbb{Z}_3 \times \mathbb{Z}_2 \times \{0\} \times \mathbb{Z}_7.$$

7.33 Poiché $\mathrm{Aut}(\mathbb{Z}_8) \cong U(\mathbb{Z}_8)$, è sufficiente trovare un isomorfismo fra il sottogruppo V di S_4 e $U(\mathbb{Z}_8)$. Si verifica facilmente che l'applicazione $f : V \to U(\mathbb{Z}_8)$ definita da $(12)(34) \mapsto [3]_8$ e $(13)(24) \mapsto [5]_8$ è un isomorfismo.

7.35 (d) Per $\mathbb{Z}_{p^\infty}$ questo segue immediatamente dal fatto che tutti i sottogruppi propri di A sono isomorfi a $\mathbb{Z}_{p^n}$, come dimostrato nell'esempio 7.21.

Sia $G = \mathbb{Q}$ e supponiamo per assurdo che H sia un sottogruppo massimale di G. Poiché H è normale in $\mathbb{Q}$, il gruppo quoziente $\mathbb{Q}/H$ è privo di sottogruppi propri e quindi ha ordine p, per qualche primo p. Allora per ogni $r \in \mathbb{Q}$, si ha $pr \in H$. Pertanto $p\frac{x}{p} = x \in H$ per ogni $x \in \mathbb{Q}$, da cui $H = \mathbb{Q}$, assurdo.

(e) Sia H un sottogruppo proprio di G. Allora esiste un elemento $x \in G$ che non appartiene ad H. Il sottogruppo ciclico $\langle x \rangle$ non ha sottogruppo propri, quindi $x \notin H$ implica $\langle x \rangle \cap H = \{0\}$. Ora per il lemma 6.47 esiste un sottogruppo M contenente H con $\langle x \rangle \cap M = \{0\}$ e massimale con queste due proprietà. Non è difficile vedere che M è un sottogruppo massimale di G.

(f) Segue dal teorema di corrispondenza.

7.36 Sia M un sottogruppo massimale di G. Allora il quoziente G/M non ha sottogruppi propri non banali, quindi $G/M \cong \mathbb{Z}_p$ per qualche primo p. Questo implica $pG \leq M$, quindi pG è proprio. Questo dimostra che (a) implica (b), mentre (b) e (c) sono equivalenti.

Supponiamo ora che valga (b). Il quoziente $G_1 = G/pG$ è un gruppo abeliano che soddisfa le ipotesi del punto (e) dell'esercizio 7.35. Pertanto G_1 possiede un sottogruppo massimale M. Per (f) dell'esercizio 7.35 anche il gruppo G possiede un sottogruppo massimale.

7.37 Diremo che un gruppo abeliano ha la proprietà $\mathcal{P}$ se ogni sottogruppo proprio di G è finito. Tutti i gruppi finiti soddisfano $\mathcal{P}$. D'altra parte, se ogni sottogruppo di G è un addendo diretto di G, allora G soddisfa $\mathcal{P}$ se e solo se G è finito. Sia G gruppo abeliano infinito che soddisfa $\mathcal{P}$, allora tutti i sottogruppi e tutti i quozienti di G

soddisfano $\mathcal{P}$. Poiché $\mathbb{Z}$ non soddisfa $\mathcal{P}$, G non è un gruppo ciclico infinito e quindi tutti gli elementi di G hanno periodo finito. Sia p un numero primo: denotiamo con G_p il sottogruppo di G formato da tutti gli elementi con periodo potenza di p. Allora tutti i sottogruppi G_p di G sono finiti. Poiché G è infinito, esiste una successione di primi tra loro distinti $p_1, p_2, \dots, p_n, \dots$ tali che $G_{p_n} \neq 0$ per ogni n. Poiché un elemento non nullo x di G_{p_1} non può appartenere al sottogruppo H generato da $G_{p_2}, G_{p_2}, \dots, G_{p_n}, \dots$, concludiamo che H è proprio, e quindi finito. Poiché il sottogruppo generato da $G_{p_2}, G_{p_3}, \dots, G_{p_n}$ ha ordine almeno $p_2 \cdots p_n$, si ha $G_p \neq 0$ solo per un numero finito di primi p. Allora uno di questi sottogruppi, diciamo G_p è infinito, pertanto $G = G_p$ perché G soddisfa $\mathcal{P}$. Adesso consideriamo il sottogruppo $pG = \{px : x \in G\}$ di G. Il quoziente G/pG soddisfa $\mathcal{P}$. D'altra parte, ogni sottogruppo di G/pG è un addendo diretto di G/pG per l'esempio 6.48. Quindi G/pG è finito. Poiché G è infinito, concludiamo che anche il sottogruppo pG è infinito. Ma allora $pG = G$. Ora scegliamo arbitrariamente un elemento non nullo c_1 di G con $o(c_1) = p$. Dall'uguaglianza $pG = G$ troviamo un elemento $c_2 \in G$ tale che $pc_2 = c_1$ e $o(c_2) = p^2$. Costruiamo per induzione su n una successione di elementi c_n di G tali che $pc_n = c_{n-1}$ per $n \in \mathbb{N}_+$. Allora i sottogruppi $C_n = \langle c_n \rangle$ di G formano una catena con $G = \bigcup_{n=1}^{\infty} C_n$ poiché tale catena è propriamente crescente e G soddisfa $\mathcal{P}$. Da qui si deduce che $G \cong \mathbb{Z}_{p^\infty}$.

13.8 Esercizi del capitolo 8

8.1 Supponiamo che G non sia abeliano e che $1 \neq a$ sia un elemento di G. Allora $o(a)$ divide 6, ma non può essere 6 perché altrimenti G risulterebbe ciclico e quindi abeliano. Per il lemma di Cauchy, esistono $a, b \in G$ tali che $o(a) = 2$ e $o(b) = 3$. Sia $K = \langle b \rangle$; allora K è normale in G. Sia $H = \langle a \rangle$, se H fosse normale in G, allora G sarebbe isomorfo al prodotto diretto di un gruppo ciclico di ordine 3 e di un gruppo ciclico di ordine 2, e sarebbe pertanto ciclico di ordine 6, contro la nostra ipotesi. Poiché il cuore H_G di H è contenuto in H ed è normale in G, si ha $H_G = \{1\}$. Il numero di classi laterali di H in G è $[G : H] = 3$. Consideriamo l'azione di G sulle classi laterali di H, come descritto nell'esempio 8.35. Il nucleo dell'azione è $H_G = \{1\}$, pertanto G è isomorfo ad un sottogruppo di S_3. Poiché $|G| = 6$, si conclude $G \cong S_3$.

8.6 (a) Se $h \in H \cap Z(G)$, allora $h = h^x \in H^x$ per ogni $x \in G$.

(b) Osserviamo che H_G coincide con H quando il sottogruppo H è normale. Quindi basta trovare un esempio di un gruppo G con un sottogruppo normale proprio H che non sia contenuto nel centro di G. Per esempio $G = S_3$, $Z(G) = \{1\}$ e $H = \langle(123)\rangle$ sottogruppo normale di G.

8.8 Se $n \geq 5$, il teorema 8.27 garantisce che A_n è un gruppo semplice non abeliano e quindi $Z(A_n) = \{1\}$, si confronti anche con l'esercizio 5.32. Consideriamo quindi il caso $n = 4$. Come osservato nell'esercizio 5.39, se a, b sono due elementi di un

gruppo G tali che $ab \neq ba$, allora $a, b, a^{-1}, b^{-1}, ab, ba \notin Z(G)$. I casi $n = 3$ e 4 si verificano pertanto facilmente.

8.10 Poiché per ipotesi H non è un sottogruppo normale di G, $N_G(H)$ è un sottogruppo proprio di G. In particolare, $[G : N_G(H)] > 1$. Per l'esercizio 5.41

$$[G : H] = [G : N_G(H)][N_G(H) : H],$$

quindi l'ipotesi $[G : H] = p$ implica che $[N_G(H) : H] = 1$, cioè $N_G(H) = H$.

8.12 Si osservi che il numero dei sottogruppi coniugati H^x di H coincide con l'indice $[G : N_G(H)]$ per il lemma 8.20. In particolare, poiché $H \leq N_G(H)$ e di conseguenza $[G : N_G(H)] \leq [G : H]$, ci sono al più $[G : H]$ sottogruppi coniugati H^x di H. Per concludere si noti che l'unione $\bigcup_{x \in G} H^x$ non è disgiunta perché 1 appartiene a tutti i sottogruppi. Quindi la cardinalità dell'unione è strettamente minore di

$$|H| \cdot [G : N_G(H)] \leq |H| \cdot [G : H] = |G|.$$

8.13 Supponiamo che $\mathrm{Aut}(G)$ sia ciclico. Allora anche il gruppo $G/Z(G)$ è ciclico in quanto isomorfo al sottogruppo $\mathrm{Inn}(G)$ di $\mathrm{Aut}(G)$ per il lemma 6.26. Il lemma 8.15 implica che G è abeliano, assurdo.

8.14 Supponiamo che $\mathrm{Aut}(G) \cong \mathbb{Z}$ per qualche gruppo G. Allora G è abeliano per l'esercizio 8.13. Se esiste un elemento $x \in G$ che non ha periodo al più 2, allora $-id_G$ definito da $x \mapsto -x$ è un automorfismo di periodo 2, mentre $\mathbb{Z}$ non ha elementi di periodo 2. Quindi vale $2x = 0$ per tutti gli elementi di G. Osserviamo che G non può essere ciclico perché $\mathrm{Aut}(\mathbb{Z}_2)$ è banale. Allora G contiene almeno 2 elementi non nulli, e il sottogruppo H da essi generato è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Per l'esempio 6.48 esiste un sottogruppo N di G tale che $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times N$. Quindi $\mathrm{Aut}(G)$ contiene un sottogruppo isomorfo a $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong GL_2(\mathbb{F}_2)$. Poiché questo gruppo non è abeliano, anche $\mathrm{Aut}(G)$ risulta non abeliano, assurdo.

8.15 Supponiamo che $\mathrm{Aut}(G) \cong \mathbb{Z}_m$ per qualche gruppo G. Allora G è abeliano per l'esercizio 8.13. Se esiste un elemento $x \in G$ che non ha periodo al più 2, allora $-id_G$ definito da $x \mapsto -x$ è un automorfismo di periodo 2, mentre $\mathbb{Z}_m$ non ha elementi di periodo 2. Quindi vale $2x = 0$ per tutti gli elementi di G. Ora si conclude come nello svolgimento dell'esercizio 8.14.

8.18 Siano $\tau = (12)$, $\sigma = (1234)$ e $H = \langle \tau, \sigma \rangle$. Allora H contiene anche le trasposizioni $(23) = \tau^{\sigma^3}$, $(34) = \tau^{\sigma^2}$ e $(14) = \tau^{\sigma}$. Quindi H contiene il sottogruppo

$$V = \{id, (12)(34), (13)(24), (14)(23)\}$$

di A_4. Essendo $(123) = (12) \circ (23) \in H$, anche $A_4 = \langle (123), V_4 \rangle$ è contenuto in H. Ora $S_4 = \langle \tau, H \rangle = H$.

8.19 Osserviamo che S_4/V è un gruppo non abeliano di ordine 6 e quindi per l'esercizio 8.1 esiste un isomorfismo $g : S_4/V \to S_3$. Definiamo $f : S_4 \to S_3$ come la

composizione $f = g \circ \pi$ ove $\pi : S_4 \to S_4/V$ è la proiezione canonica sul quoziente. Allora f è un omomorfismo suriettivo con $\ker f = V$.

8.20 Denotando i vertici del quadrato dell'esercizio 5.51 con 1, 2, 3 e 4, notare che la rotazione σ corrisponde al ciclo (1234), mentre il ribaltamento del quadrato rispetto alla diagonale 24 corrisponde alla trasposizione (13).

8.21 Il gruppo A_4 ha 8 elementi di ordine 3 e 3 elementi di ordine 2 che sono $(12)(34), (13)(24)$ e $(14)(23)$. Questi elementi generano un sottogruppo V di ordine 4. Più precisamente ogni coppia di elementi distinti x e y di ordine 2 genera V. In altre parole un sottogruppo H di ordine 6 di A_4 non può contenere più di un elemento di ordine 2. D'altra parte H non può essere abeliano, perché altrimenti sarebbe ciclico e quindi A_4 avrebbe un elemento di ordine 6, assurdo. Quindi H deve essere non abeliano. Per l'esercizio 8.1 $H \cong S_3$ deve avere almeno due elementi di ordine 2, assurdo. Si potrebbe evitare il ricorso all'esercizio 8.1 notando che se $x \in H$ ha $o(x) = 3$, allora l'elemento h di H di ordine 2 insieme a x genera un sottogruppo di H che contiene tutto il sottogruppo V. Infatti, poiché x e h non commutano, gli elementi h, h^x, h^{x^2} sono distinti elementi di H di periodo 2, di conseguenza H contiene tutti gli elementi di periodo 2 di A_4 che formano il sottogruppo V.

8.22 Poiché $\sigma = (123)(456)(789), \tau = (147)(258)(369)$,

$$\sigma \circ \tau = \tau \circ \sigma = (159)(267)(348)$$

si ha $o(\sigma) = o(\tau) = o(\sigma\tau) = 3$.

Osserviamo che $\langle\sigma\rangle \cong \langle\tau\rangle \cong \mathbb{Z}_3$ e $H \cong \langle\sigma\rangle \times \langle\tau\rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Allora H è abeliano, non ciclico di ordine 9.

8.24 Ragionare per induzione su n. Il caso $n = 1$ è banale. Se $n > 1$, $|G| = p^n$ e d è un divisore di $|G|$, si usi il fatto che il centro $Z(G)$ è non banale. Si scelga un elemento $z \in Z(G)$ di ordine p. Il sottogruppo $H = \langle z\rangle$ è centrale, quindi normale. Al gruppo quoziente $G_1 = G/H$ e $d' = d/p$ si applichi l'ipotesi induttiva, in quanto $|G_1| = p^{n-1}$ e d' divide $|G_1|$, per trovare un sottogruppo K di G_1 di ordine d'. L'immagine inversa L di K tramite l'omomorfismo canonico $G \to G/H$ soddisfa $|L| = p|K| = d$.

8.25 (a) Innanzitutto il centro $Z = Z(GL_2(\mathbb{R})) \cong (\mathbb{R}^*, \cdot)$ per il lemma 5.74 d). Il sottogruppo N^+ di B_2^+ formato delle matrici $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G$ è un sottogruppo normale di B_2^+ isomorfo a $(\mathbb{R}, +)$. Ora basta notare che $B_2^+ = Z \cdot N^+$ e $N^+ \cap Z = \{I_2\}$.

(b) è ovvio.

Per provare (c) si consideri una matrice $U = (u_{ij})$ dell'intersezione $H \cap H^x$. Coniugando con la matrice x si ha

$$x^{-1}\begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} x = \begin{pmatrix} u_{11} - ru_{21} & ru_{11} - r^2u_{21} + u_{12} - ru_{22} \\ u_{21} & u_{22} + ru_{21} \end{pmatrix} \in H.$$

Ora $u_{22} + ru_{21} \in \mathbb{Q}$ implica $u_{21} = 0$. Similmente $ru_{11} - r^2u_{21} + u_{12} - ru_{22} \in \mathbb{Q}$ implica $u_{11} = u_{22}$. Quindi U è del tipo richiesto. Un argomento simile funziona per i casi $H \cap H^y$, $H \cap H^z$ e $H \cap H^u$.

(d) Basta notare che $B_2^+ \cap B_2^- = Z(GL_2(\mathbb{R}))$.

8.26 (d) Sia r un numero reale irrazionale e $z = \begin{pmatrix} r^{-1} & 0 \\ 0 & 1 \end{pmatrix}$. Supponiamo di avere $z^{-1}wz \in H_1$ per qualche $w = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \in H_1$. Allora $v \in \mathbb{Q}$ e

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & rv \\ 0 & 1 \end{pmatrix} \in H_1.$$

Quindi $vr \in \mathbb{Q}$. Poiché $v \in \mathbb{Q}$ e $r \notin \mathbb{Q}$, questo è possibile solo se $v = 0$. Allora $w = I_2$ e di conseguenza $H_1 \cap H_1^z = \{I_2\}$.

(e) Sia $x = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ con r numero reale irrazionale. Per l'esercizio 8.25, l'intersezione $H \cap H^x$ è contenuta nel sottogruppo B_2^+ di $GL_2(\mathbb{R})$, quindi anche nel sottogruppo

$$N^+ = G \cap B_2^+.$$

Poiché H è contenuto anche in $GL_2(\mathbb{Q})$, per il punto (c) dell'esercizio 8.25 si ha $H \cap H^z \leq D_2$. Pertanto

$$H \cap H^x \cap H^z \leq N^+ \cap D_2 = \{I_2\}.$$

8.27 (c) Notiamo che per ogni $r \in \mathbb{R}^*$ le matrici $x = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ e $u = \begin{pmatrix} r^{-1} & 0 \\ 0 & r \end{pmatrix}$ appartengono al sottogruppo $SL_2(\mathbb{R})$ e quindi si può applicare direttamente l'esercizio 8.25.

8.29 Per l'esercizio 8.25 esiste $x \in G$ tale che $H \cap H^x \leq B_2^+$ ed esiste $z \in G$ tale che $H \cap H^z \leq D_2$. Quindi $H \cap H^x \cap H^z \leq B_2^+ \cap D_2 = Z(G)$.

8.30 Dimostriamo la proprietà riflessiva: poiché f è un omomorfismo, $f(1) = id_\Omega$ e quindi $x^1 = x$ per ogni $x \in \Omega$. Analogamente si dimostrano le proprietà simmetrica e transitiva, utilizzando il fatto che f è un omomorfismo.

8.32 (a) Se per assurdo H non è normale in G, allora $N_G(H) < G$ e quindi $N_G(H) = H$. Allora, grazie al lemma 8.20, l'insieme X dei coniugati di H contiene 3 elementi. Sia dunque

$$X = \{H, H^a, H^b\}.$$

Per ogni $g \in G$ si definisca l'applicazione $\varphi_g : X \to X$ con $\varphi_g(x) = x^{g^{-1}}$. Si dimostri che φ_g è biettiva, cioè $\varphi_g \in S_X$ per ogni $g \in G$. Si consideri ora l'applicazione $\varphi : G \to S_X$ tale che $\varphi(g) = \varphi_g$ e si dimostri che è un omomorfismo di gruppi con nucleo H_G. Si ricordi che $H_G \triangleleft G$ e $H_G \leq H$. Per il primo teorema di omomorfismo, G/H_G è isomorfo ad un sottogruppo non banale di $S_X = S_3$. Inoltre per l'esercizio 5.41 abbiamo

$$|G/H_G| = [G : H_G] = [G : H] \cdot [H : H_G] = 3 \cdot [H : H_G].$$

Essendo G di ordine dispari, concludiamo che anche $[H : H_G]$ è dispari. D'altra parte $|G/H_G|$ divide l'ordine di S_3. Quindi $3 \cdot [H : H_G]$ divide 6. Questo implica $[H : H_G] = 1$ e di conseguenza $H = H_G \lhd G$, che contraddice l'ipotesi fatta.

(b) Si consideri il gruppo $G = S_3$ e il suo sottogruppo $H = \langle (12) \rangle$ di indice 3, che non è normale.

(c) Utilizzando l'esercizio 5.41, è noto che

$$[G : H] = p = [G : K][K : H],$$

da cui segue che $K = G$ oppure $K = H$.

8.43 Sia $\Omega = \{X \subseteq G : |X| = p^a\}$. Allora

$$|\Omega| = \binom{n}{p^a} = \binom{p^a m}{p^a} \equiv_p m$$

per l'esercizio 3.63. Quindi $|\Omega|$ non è divisibile per p. Consideriamo l'azione di G su se stesso per moltiplicazione a sinistra, come definita nell'esempio 8.32 e la relativa azione su Ω, come descritta nell'esempio 8.37. Dal fatto che Ω è finito, segue che c'è un numero finito di orbite $\Delta_1, \dots, \Delta_r$ rispetto a questa azione. Poiché p non divide $|\Omega|$ e

$$|\Omega| = \sum_{i=1}^{r} |\Delta_i|,$$

esiste un orbita Δ_i per qualche $i = 1, \dots, r$ tale che p non divide $|\Delta_i|$. Sia $X \in \Delta_i$; allora per il lemma 8.36, si ha che p non divide $[G : G_X]$. Per il teorema di Lagrange 5.52 si ha che p^a divide $|G_X|$. Sia ora $x \in X$. Allora $G_X x = \{gx : g \in G_X\}$ è contenuto in X per la definizione dello stabilizzatore G_X e quindi

$$|G_X| = |G_X x| \leq |X| = p^a.$$

Concludiamo che G_X è un sottogruppo di ordine p^a.

8.44 (a) Poiché BB^{-1} non è grande a sinistra, possiamo costruire per induzione su n una successione di elementi $e = g_0, g_1, g_2, \dots, g_n$ di G tale che $g_n \notin \bigcup_{k=1}^{n-1} g_k BB^{-1}$. In altre parole, $g_k B \cap g_n B = \emptyset$ per tutti i $k < n$.

(b) Essendo S finito, l'insieme SS^{-1} non è grande a sinistra e si applica (a). Si dimostra analogamente che S è piccolo a destra.

8.45 Osserviamo che H è grande a sinistra (o destra) se e solo se H ha indice finito in G. Questo dimostra l'equivalenza di (a), (b) e (c). Poiché $H = HH^{-1} = H^{-1}H$, dall'esercizio 8.44 (a) si ricava che (b) è equivalente a (d) e (c) è equivalente ad (e).

8.46 (a) Se l'orbita $\mathcal{O}_s$ è infinita, l'asserto è ovvio. Se $|\mathcal{O}_s| < \infty$, allora $H = G_s$ è infinito, e quindi $H \subseteq \{g \in G : g.s \notin F\}$ è infinito.

(b) è ovvio e (c) segue da (b).

(d) Secondo (c) e l'ipotesi, l'insieme $M = \{g \in G : S \cap g.S \neq \emptyset\}$ è finito. Per l'esercizio 8.44 (b) esistono elementi $g_1, g_2, \dots, g_n, \dots$ a due a due distinti del

gruppo tali che $g_n M \cap g_m M = \emptyset$ qualora $m \neq n$, in altre parole $g_m^{-1} g_n \notin MM^{-1}$. Poiché $e \in M$ si ha $g_m^{-1} g_n \notin M$, e quindi $((g_m^{-1} g_n).S) \cap S = \emptyset$, qualora $m \neq n$. Quindi $(g_n.S) \cap (g_m.S) = \emptyset$ qualora $m \neq n$.

(e) Se $|G_x| < \infty$ per ogni $x \in S$, allora troviamo $g_1, g_2, \ldots, g_n, \ldots$ come nel punto (d). Essendo gli insiemi $g_n.S$ a due a due disgiunti, solo un numero finito di essi possono intersecare F. Quindi tutti i g_n, a meno di un numero finito, appartengono ad A.

Supponiamo adesso che esista $s \in S$ con G_s infinito. Proviamo l'asserto per induzione su $n = |S|$. Se $n = 1$, allora $H_s \subseteq A$ e l'asserto è provato. Supponiamo $n > 1$ e che l'asserto sia vero per tutte le azioni di un gruppo G su un insieme infinito X e per tutte le coppie di insiemi finiti disgiunti S, F di X con $|S| \leq n - 1$. Ora G_s agisce su X e per gli insiemi finiti disgiunti $S_1 = S \setminus \{s\}$ e F di X esistono infiniti $h \in G_s$ con $(h.S_1) \cap F = \emptyset$. Poichè $h.s = s$ per ogni $h \in G_s$ e $S \cap F = \emptyset$, si ha anche $(h.S) \cap F = \emptyset$.

13.9 Esercizi del capitolo 9

9.6 Fissiamo prima q_1 e notiamo che $L(q_1) = \{q \in \mathbb{H} : \overline{q_1 q} = \overline{q}\,\overline{q_1}\}$ è un sottospazio di $\mathbb{H}$ che contiene $\mathbb{R}$. Analogamente, fissando q_2 si nota che $R(q_2) = \{q \in \mathbb{H} : \overline{q q_2} = \overline{q_2}\,\overline{q}\}$ è un sottospazio di $\mathbb{H}$ che contiene $\mathbb{R}$. Osserviamo che $i, j, k \in L(i)$ e quindi $L(i) = \mathbb{H}$. Questo vuol dire che in particolare $q_2 \in L(i)$, ovvero $i \in R(q_2)$. Analogamente si conclude che $j, k \in R(q_2)$. Essendo $R(q_2)$ un sottospazio di $\mathbb{H}$ contenente $\mathbb{R}$ si conclude $R(q_2) = \mathbb{H}$ e quindi anche $q_1 \in R(q_2)$. Questo dimostra $\overline{q_1 q_2} = \overline{q}_2 \overline{q}_1$.

9.7 Per provare $\|q_1 q_2\| = \|q_1\| \|q_2\|$ notiamo che basta verificare $\|q_1 q_2\|^2 = \|q_1\|^2 \|q_2\|^2$. Questa uguaglianza è equivalente all'uguaglianza

$$q_1 q_2 \overline{q_1 q_2} = q_1 \overline{q_1} \|q_2\|^2. \tag{$*$}$$

Se $q_1 = 0$, (*) è stata verificata. Se $q_1 \neq 0$, (*) è equivalente all'uguaglianza $q_2 \overline{q_1 q_2} = \overline{q_1} \|q_2\|^2$. Come abbiamo già visto, vale $\overline{q_1 q_2} = \overline{q}_2 \overline{q}_1$. Quindi basta notare che la parte a sinistra $q_2 \overline{q}_2 \overline{q}_1$ si può scrivere anche come $\|q_2\|^2 \overline{q_1}$ e pertanto coincide con $\overline{q_1} \|q_2\|^2$ in quanto $\|q_2\|^2$ è un numero reale e quindi commuta con $\overline{q_1}$.

9.8 (a) Se $q_1 q_0 = q_0 q_1$ e $q_2 q_0 = q_0 q_2$, allora anche $(q_1 - q_2) q_0 = q_0 (q_1 - q_2)$ e $(q_1 q_2) q_0 = q_1 q_0 q_2 = q_0 q_1 q_2$. Quindi $q_1 - q_2 \in B(q_0)$ e $q_1 q_2 \in B(q_0)$ quando $q_1, q_2 \in B(q_0)$. Poiché $0 \in B(q_0)$, questo dimostra che $B(q_0)$ è un sottoanello di $\mathbb{H}$. Se $q \in B(q_0)$ e $q \neq 0$, allora da $q q_0 = q_0 q$ deduciamo che $q^{-1} q_0 = q_0 q^{-1}$, e quindi $q^{-1} \in B(q_0)$. Pertanto $B(q_0)$ è un corpo.

(b) Si ha $\mathbb{R} \subseteq B(q_0)$, perciò $B(q_0)$ risulta stabile per la moltiplicazione per $r \in \mathbb{R}$, essendo un sottoanello di $\mathbb{H}$. Pertanto $B(q_0)$ è sottospazio vettoriale di $\mathbb{H}$.

(c) Per $q_0 \in \mathbb{R}$ vale $B(q_0) = \mathbb{H}$. Supponiamo ora $q_0 = a_0 + b_0 i + c_0 j + d_0 k \notin \mathbb{R}$, con $a_0, b_0, c_0, d_0 \in \mathbb{R}$. Dimostreremo che $B(q_0) = \mathbb{R} + \mathbb{R} q_0$. Sia $q' = Im(q_0) =$

$q_0 - a_0$. Chiaramente, $B(q') = B(q_0)$ e $\mathbb{R} + \mathbb{R}q_0 = \mathbb{R} + \mathbb{R}q'$. Pertanto possiamo supporre che $a_0 = 0$, cioè $q_0 = b_0 i + c_0 j + d_0 k \neq 0$. Se adesso $q = a + bi + cj + dk \in B(q_0)$, allora anche $q^* = q - a \in B(q_0)$. Da $q_0 q^* = q^* q_0$ ricaviamo

$$-(b_0 b + c_0 c + d_0 d) + (c_0 d - d_0 c)i + (d_0 b - b_0 d)j + (b_0 c - c_0 b)k =$$

$$-(b_0 b + c_0 c + d_0 d) - (c_0 d - d_0 c)i - (d_0 b - b_0 d)j - (b_0 c - c_0 b)k.$$

Questo è possibile se e solo se $c_0 d - d_0 c = d_0 b - b_0 d = b_0 c - c_0 b = 0$. Quindi da $q_0 \neq 0$ concludiamo che esiste un numero reale r tale che $b = rb_0$, $c = rc_0$ e $d = rd_0$. Pertanto $q^* = rq_0$ e quindi $q = a + rq_0 \in \mathbb{R} + \mathbb{R}q_0$.

(d) L'asserto segue immediatamente dal fatto che $B(q_0) \supseteq \mathbb{R} + \mathbb{R}q_0$ e $\overline{q} \in \mathbb{R} + \mathbb{R}q_0$ per ogni $q \in \mathbb{R} + \mathbb{R}q_0$.

(e) Da (c) segue che $B(q_0) = \mathbb{H}$ se e solo se $B(\overline{q_0}) = \mathbb{H}$ (se e solo se $q_0 \in \mathbb{R}$). Altrimenti si ragiona come in (c) notando che $q \in \mathbb{R} + \mathbb{R}q_0$.

9.11 Rispettivamente: 30, 48, 72 e 96.

9.12 (b) $\to$ (a) L'uguaglianza $\|q_1\| = \|q_2\|$ è soddisfatta se $q_2 = q_0 q_1 q_0^{-1}$ per qualche q_0. L'uguaglianza $Re(q_1) = Re(q_2)$ si prova facilmente ricordando che $q_0^{-1} = \|q_0\|^{-1}\overline{q}_0$.

(a) $\to$ (b) Se $q_2 = q_1$ vale $q_2 = q_0^{-1} q_1 q_0$ con $q_0 = 1$. Nel seguito supponiamo $q_2 \neq q_1$.

(1) Consideriamo il caso $Re(q) = Re(q_1) = 0$. Supponiamo dapprima $q_2 \neq -q_1$ e quindi $q_0 = q_1 + q_2 \neq 0$. Da $Re(q) = Re(q_1) = 0$ e $\|q_1\| = \|q_2\|$ deduciamo $q_1^2 = -\|q_1\|^2 = -\|q_2\|^2 = q_2^2$. Da questo segue immediatamente che $q_0 q_2 = q_1 q_0$. Quindi vale $q_2 = q_0^{-1} q_1 q_0$.

Se $q_2 = -q_1 \neq 0$ possiamo trovare $q_0 = b_0 i + c_0 j + d_0 k \neq 0$ con

$$b_1 b_0 + c_1 c_0 + d_1 d_0 = 0, \text{ dove } b_1 i + c_1 j + d_1 k = q_1.$$

Non è difficile vedere che $q_1 q_0 = -q_0 q_1 = q_0 q_2$. Pertanto $q_2 = q_0^{-1} q_1 q_0$.

(2) Nel caso generale poniamo $a_i = Re(q_i)$ per $i = 1, 2$ e notiamo che i quaternioni $\tilde{q}_i = q_i - a_i$ soddisfano $Re(\tilde{q}_1) = Re(\tilde{q}_2) = 0$ e $\|\tilde{q}_1\| = \|\tilde{q}_2\|$. Pertanto esiste un quaternione $q_0 \neq 0$ tale che $\tilde{q}_2 = q_0^{-1} \tilde{q}_1 q_0$. Da questo segue immediatamente che $q_2 = q_0^{-1} q_1 q_0$, dato che $a_1 = a_2$ per ipotesi.

9.13 (c) Basta vedere che ogni sottogruppo normale non centrale N di S coincide con S.

Sia $Re(N) = \{a \in \mathbb{R} : Re(q) = a \text{ per qualche } q \in N\}$. Per l'esercizio 9.12 se $Re(q) \in Re(N)$ per qualche $q \in S$, allora anche $q \in N$. Quindi basta dimostrare che $Re(N) = [-1, 1]$.

Notiamo che se $q \in S$, allora $Re(q^2) = 2Re(q)^2 - 1$. Questo suggerisce di introdurre la funzione $f(x) = 2x^2 - 1$ da $[-1, 1]$ a $[-1, 1]$.

(i) Se $a \in Re(N)$, allora $[f(a), 1] \subseteq Re(N)$.

Se $b \in [f(a), 1]$ dobbiamo dimostrare che N contiene un quaternione q con $Re(q) = b$. Supponiamo $a \neq \pm 1$ e quindi $\left|\frac{b - a^2}{1 - a^2}\right| \leq 1$ da cui segue che possiamo scegliere $\varphi \in [0, 2\pi]$ con $b = a^2 - (1 - a^2)\cos\varphi$. Poniamo

$$q_1 = a + \sqrt{1-a^2}i \quad \text{e} \quad q_2 = a + \sqrt{1-a^2}(\cos\varphi i + \sin\varphi j).$$

Si ha $q_1, q_2 \in S$. Da $Re(q_j) = a \in Re(N)$ per $j = 1, 2$ segue $q_1, q_2 \in N$ e quindi $q_1 q_2 \in N$. Ora $b = a^2 - (1-a^2)\cos\varphi = Re(q_1 q_2) \in Re(N)$.

(ii) Se $0 \in Re(N)$, allora $N = S$. Infatti con $a = 0$ dal punto (i) segue $[-1, 1] \subseteq Re(N)$. Quindi $N = S$.

Ora consideriamo il caso generale. Essendo N non centrale esiste $a \in Re(N)$, $a \neq \pm 1$. Per (i), si ha che $a \in Re(N)$ implica $f(a) \in Re(N)$, da cui per induzione ancora applicando (i), si ottiene $[f^m(a), 1] \subseteq Re(N)$ per ogni $m \in \mathbb{N}_+$.

Osserviamo che $f(x) < x$ per ogni $x \in \,]-\frac{1}{2}, 1[$. Se $f(a) \leq 0$, allora $0 \in [f(a), 1] \subseteq Re(N)$ e (ii) implica $N = S$.

Passiamo al caso $1/\sqrt{2} < f(a) < a \leq 1$. Se $f(f(a)) \leq 1/\sqrt{2}$ ragioniamo come prima con $a_1 = f(a)$ al posto di a e proviamo $N = S$. Quindi possiamo assumere che

$$1/\sqrt{2} < f(f(a)) < f(a) < a < 1. \qquad (\dagger)$$

Notiamo che $f(x) \leq x$ per tutti gli $x \in [0, 1]$. Inoltre, se $1/\sqrt{2} < x < y \leq 1$, si ha

$$f(y) - f(x) = 2(y^2 - x^2) = 2(x+y)(y-x) > y - x.$$

Quindi $f(a) - f(f(a)) \geq a - f(a)$, cioè la successione $a_k = f^k(a) - f^{k+1}(a)$ è crescente per tutti i k per i quali $f^k(a) > 1/\sqrt{2}$. Di conseguenza, da ($\dagger$) esiste un $k \geq 2$ tale che $f^{k+1}(a) \leq 1/\sqrt{2} < f^k(a)$. Questo implica

$$0 = f(1/\sqrt{2}) \in [f^{k+2}(a), f^{k+1}(a)]$$

e di conseguenza $0 \in Re(N)$ per (*). Ora (ii) implica $N = S$.

9.14 Per (a) si consideri l'insieme B di tutte le somme della forma

$$k_1 a + k_2 a^2 + \ldots + k_n a^n,$$

dove $k_1, k_2, \ldots, k_n \in \mathbb{Z}$. Per (b) si consideri l'insieme C di tutte le somme della forma

$$k_{1,0}a + k_{0,1}b + k_{2,0}a^2 + k_{1,1}ab + k_{0,2}b^2 + \ldots + k_{n,0}a^n + k_{n-1,1}a^{n-1}b + \ldots + k_{0,n}b^n,$$

dove $k_{i,j} \in \mathbb{Z}$, per $i, j = 0, 1, \ldots, n$.

Nel caso in cui A è unitario, ogni sottoanello contiene il sottoanello fondamentale di A. Quindi ora vanno considerate tutte le somme della forma

$$k_0 1_A + k_1 a + k_2 a^2 + \ldots + k_n a^n,$$

dove

$$k_0, k_1, k_2, \ldots, k_n \in \mathbb{Z},$$

per ottenere il sottoanello di A generato da a. Modifica analoga si fa anche nel caso del sottoanello generato da $a, b \in A$.

9.19 (b) L'elemento (x, y) è divisore dello zero se e solo se $y = \pm x$, altrimenti è invertibile. Questo risponde anche a (c).

(d) I sottogruppi $I_1 = \{(x, x) : x \in \mathbb{R}\}$ e $I_2 = \{(x, -x) : x \in \mathbb{R}\}$ di $\mathbb{R}^2$ sono ideali principali: $I_1 = ((1, 1))$ e $I_2 = ((1, -1))$. Essendo $A/I_1 \cong A/I_2 \cong \mathbb{R}$ un campo, entrambi gli ideali sono massimali. Per il punto (c) tutti i divisori dello zero sono contenuti in $I_1 \cup I_2$ e il complemento $A \setminus (I_1 \cup I_2)$ consiste solo di elementi invertibili. Quindi gli unici ideali non banali di A sono I_1 e I_2.

9.20 La verifica che $R[G]$ è un anello è facile.

(a) Sia $e = g_1$ l'elemento neutro di G. Allora $1_A e$ è l'unità di $R[G]$.

(b) Sia e l'elemento neutro di G e $e \neq g \in G$ e poniamo $k = o(g)$. Allora gli elementi

$$x = g - e \qquad \text{ed} \qquad y = g^{k-1} + g^{k-2} + \ldots + g + e$$

di $R[G]$ sono non nulli e $xy = 0$.

9.21 Basta vedere che per due sottoanelli B e C l'estremo superiore $B \vee C$ coincide con il sottoanello generato da B, C e l'estremo inferiore $B \wedge C$ coincide con $B \cap C$.

9.22 (a) Dimostriamo che se $a + n\mathbb{Z}$ è nilpotente, allora $p_1 \ldots p_t$ divide a. Infatti, sia $(a + n\mathbb{Z})^m = n\mathbb{Z}$ per qualche $m \in \mathbb{N}$. Allora $a^m \in n\mathbb{Z}$, quindi $n = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ divide a^m e pertanto p_i divide a^m per ogni $i = 1, \ldots, t$, ossia $p_1 \ldots p_t$ divide a. Viceversa, se $p_1 \ldots p_t$ divide a, sia $\alpha = \max\{\alpha_1, \ldots, \alpha_t\}$. Allora $(p_1 \ldots p_t)^\alpha$ divide a^α, e poiché $\alpha_i \leq \alpha$, $p_i^{\alpha_i}$ divide p_i^α e quindi $p_i^{\alpha_i}$ divide a^α, per ogni $i = 1, \ldots, t$, e $n = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ divide a^α. Allora $a^\alpha \in n\mathbb{Z}$, ossia $(a + n\mathbb{Z})^\alpha = n\mathbb{Z}$ e pertanto $a + n\mathbb{Z}$ è nilpotente.

(b) Per (a) l'insieme degli elementi nilpotenti di $\mathbb{Z}/n\mathbb{Z}$ è l'ideale principale $(p_1 \ldots p_t + n\mathbb{Z})$.

9.24 Sia I l'intersezione di tutti gli ideali primi di A. Se P è un ideale primo e $a \in N(A)$, allora esiste $n \in \mathbb{N}$ tale che $a^n = 0 \in P$, quindi $a \in P$. Questo dimostra l'inclusione $I \supseteq N(A)$. Supponiamo che $x \notin N(A)$ per un certo elemento x di A. La famiglia $\mathcal{I}$ degli ideali propri di A che non intersecano l'insieme

$$S = \{x^n : n \in \mathbb{N}\}$$

non è vuoto, per esempio l'ideale (0) appartiene a $\mathcal{I}$. Si verifica facilmente, seguendo la dimostrazione del teorema di Krull, che l'insieme ordinato $(\mathcal{I}, \subseteq)$ risulta induttivo. Pertanto $\mathcal{I}$ contiene un elemento massimale M. Si verifica che M è un ideale primo. Essendo $x \notin M$, questo dimostra che $x \notin I$.

9.25 (a) Sia P un ideale primo di A. Allora il quoziente A/P è un dominio. Per il lemma 9.9, A/P è un campo. Quindi P è massimale.

(b) Essendo $N(A)$ finito possiamo scriverlo come $N(A) = \{a_1, a_2, \ldots, a_s\}$. Esistono $k_1, k_2, \ldots, k_s \in \mathbb{N}$ tali che $a_j^{k_j} = 0$ per $j = 1, 2, \ldots, s$. Non è difficile dimostrare per induzione su s che $k = k_1 + k_2 + \ldots + k_s$ è tale che $x^k = 0$ per ogni elemento x di $N(A)$.

9.26 Supponiamo $a^m = b^m$ e $a^n = b^n$ per $(m, n) = 1$ Vogliamo dimostrare che se $a \neq b$, allora a e b sono divisori di zero. Supponiamo quindi $a \neq b$. Poiché $(m, n) = 1$, esistono $x, y \in \mathbb{Z}$ tali che $1 = mx + ny$. Non possiamo avere $x > 0$ e $y > 0$. Supponiamo $x > 0$ e $y < 0$, allora $-y = z > 0$ e $1 + nz = mx$. Quindi

$$b \cdot b^{nz} = b^{mx} = a^{mx} = a^{1+nz} = a \cdot a^{nz} = a \cdot b^{nz}$$

e dunque

$$(b - a) \cdot b^{nz} = 0.$$

Analogamente si ricava $a^{nz} \cdot (a - b) = 0$. Se $a - b$ non è un divisore dello 0, si conclude $b^{nz} = a^{nz} = 0$ e cioè entrambi a e b sono nilpotenti, e quindi divisori di zero. Se a non è divisore dello 0, da $a^{nz} \cdot (a - b) = 0$ si ricava $a = b$. Analogamente, se b non è divisore dello 0, concludiamo $a = b$. Quindi a e b risultano essere divisori di 0 se $a \neq b$. Si può concludere che $a = b$ se a e b non sono divisori dello 0.

9.29 (c) Poiché $A = H + K$, esistono $h \in H$, $k \in K$ tali che $1 = h + k$. Per ogni $z \in H \cap K$ si ha $z = zh + zk \in HK$.

(d) Si considerino $(\mathbb{Z}, +, *)$ con la moltiplicazione $*$ definita da $n * m = 0$, per ogni $n, m \in \mathbb{Z}$, e gli ideali $H = 2\mathbb{Z}$ e $K = 3\mathbb{Z}$.

9.30 (a) Sia M un ideale massimale di A contenente K^n. Per $a \in K$ abbiamo

$$a^n \in K^n \subseteq M.$$

Poiché ogni ideale massimale è anche primo, concludiamo che $a \in M$. Questo dimostra che $K \subseteq M$. Essendo anche K massimale, si ha $M = K$.

(b) Segue immediatamente da (a) e dal teorema di Krull.

(c) Se $h \in H$ e $k \in K$ soddisfano $h + k = 1$, elevando l'uguaglianza alla $2n$ troviamo

$$h^{2n} + \binom{2n}{1} h^{2n-1}k + \ldots + \binom{2n}{2n-1} hk^{2n-1} + k^{2n} = 1.$$

Questo dimostra che $1 \in H^n + K^n$, poiché $h^j k^{2n-j} \in H^n$ se $j \geq n$ e $h^j k^{2n-j} \in K^n$ se $j \leq n$.

(d) Se $h \in H, k \in K, j_1, j_2 \in J$ soddisfano $h + j_1 = 1$ e $k + j_2 = 1$, moltiplicando le due uguaglianze troviamo

$$hk + (hj_2 + j_1 k + j_1 j_2) = 1,$$

con

$$hk \in HK \subseteq H \cap K \qquad \text{e } hj_2 + j_1 k + j_1 j_2 \in J.$$

Ciò dimostra $(H \cap K) + J = A$.

(e) Ragionare per induzione usando (d).

9.31 Per l'esercizio 9.25, ogni ideale primo di A è massimale, pertanto

$$M_1, M_2, \ldots, M_s$$

sono tutti gli ideali primi di A. Quindi per l'esercizio 9.24

$$M_1 \cap M_2 \cap \ldots \cap M_s = N(A).$$

Abbiamo visto nell'esercizio 9.25 che esiste $m \in \mathbb{N}$ tale che che $x^m = 0$ per ogni elemento x di $N(A)$. Sia $N(A) = \{a_1, a_2, \ldots, a_t\}$. Allora in ogni prodotto di almeno mt elementi di $N(A)$ ce ne sarà almeno uno che si ripete almeno m volte, quindi il prodotto sarà uguale a zero. Questo dimostra che per $k = mt$ si ha $N(A)^k = \{0\}$. Poiché $M_1 M_2 \ldots M_s \subseteq N(A)$, questo dimostra la seconda uguaglianza. Per la prima basta applicare il punto (f) dell'esercizio 9.30.

9.32 Sia Π un insieme di primi e sia A_Π l'insieme delle frazioni $\frac{n}{m} \in \mathbb{Q}$ tali che se un primo p divide m allora $p \in \Pi$. Si verifica che A_Π è sottoanello di $\mathbb{Q}$. Per ogni A sottoanello di $\mathbb{Q}$, esiste un insieme Π di primi tali che $A = A_\Pi$. Si considera l'insieme Π dei primi p tali che $\frac{1}{p} \in A$ e si verificano le due inclusioni: $A_\Pi \subseteq A$ e $A \subseteq A_\Pi$.

9.34 (e) Siano $d = (m, n)$ e $q = m/d$. Allora $m = dq$, $n = dn'$ per qualche $n' \in \mathbb{Z}$ e $(q, n') = 1$. Dimostriamo l'inclusione $(m\mathbb{Z} : n\mathbb{Z}) \subset q\mathbb{Z}$. Se $x \in (m\mathbb{Z} : n\mathbb{Z})$, allora $\forall h \in \mathbb{Z}, x(nh) = mk$ per qualche $k \in \mathbb{Z}$. Pertanto se $h = 1$, risulta $xn' = qk$ ossia q divide x, quindi $x \in q\mathbb{Z}$. Viceversa se $x \in q\mathbb{Z}$, allora $x = qh$ per qualche $h \in \mathbb{Z}$. Sia $y \in n\mathbb{Z}, y = nk$ per qualche $k \in \mathbb{Z}$. Allora

$$xy = qh(nk) = qh(dn')k = h(qd)n'k = m(hn'k) \in m\mathbb{Z}$$

e questo prova l'inclusione opposta.

9.36 (a) Poiché $I + J = A$, esistono $x \in I$ e $y \in J$ con $x + y = 1$. Allora, per ogni $z \in I \cap J$, si ha $z = xz + zy \in IJ$.

(c) Applicare (b) con $I = J$.

(e) Se $I = (k)$ e $J = (n)$ in $A = \mathbb{Z}$, abbiamo $IJ = (kn)$ per (b) mentre $I \cap J = (m)$, dove m è il minimo comune multiplo di k e n.

Se $b \in B$, allora $b = cb^2$ per qualche elemento $c \in B$. Pertanto $(b^2) = (b)$. Quindi per ogni elemento $b \in I \cap J$ si ha $b \in (b^2) = (b)(b) \subseteq IJ$. Dunque l'uguaglianza $I \cap J = IJ$ vale sempre in questo anello.

9.37 Una matrice $\alpha \in A$ è invertibile se e solo se $a^2 + b^2 \not\equiv 0 \pmod 3$. Gli unici quadrati mod 3 sono 0 e 1, quindi ogni matrice non nulla appartenente ad A è invertibile. Inoltre A^* ha otto elementi: ci sono 3 scelte per a, 3 scelte per b ed escludiamo la scelta di a e b entrambi 0.

9.49 (b) Si ha che $\frac{m}{n}$ è invertibile se e solo se p non divide m.

(c) Sia I un ideale proprio di $\mathbb{Z}_{(p)}$. Allora I non contiene elementi invertibili. Pertanto p divide m, per ogni $\frac{m}{n} \in I$. Scegliamo $\frac{m_0}{n_0} \in I$ tale che p^k divide m e k è minimale con questa proprietà tra tutti gli $\frac{m}{n} \in I$. Allora I coincide con l'ideale principale $(\frac{m}{n}) = (p^k)$. In particolare $\mathbb{Z}_{(p)}$ è un dominio principale.

(d) Poiché $\mathbb{Z}_{(p)}$ non ha divisori di 0, in quanto sottoanello di $\mathbb{Q}$, l'ideale (0) è primo. Poiché $\mathbb{Z}_{(p)}$ è un dominio a ideali principali, un ideale non nullo $I = (p^k)$ è

primo se e solo se p^k è irriducibile. Ma questo avviene precisamente quando $k = 1$. Quindi l'unico ideale primo e non nullo è (p). Poiché $\mathbb{Z}_{(p)}/(p) \cong \mathbb{Z}_p$ è un campo, questo ideale è anche l'unico ideale massimale di $\mathbb{Z}_{(p)}$.

9.50 Per (b), applicare l'esercizio 9.48. Per l'esempio in (c) si utilizzi l'esercizio 9.49.

9.51 (a) Supponiamo che A sia un campo. Per $x \in A$ ci sono due possibilità: se $x = 0$, allora $x = yx^2$ vale per ogni $y \in A$; se

$$x \neq 0, \ x = yx^2 \text{ vale per } \ y = x^{-1}.$$

Pertanto A è regolare. Ora supponiamo che A sia un dominio regolare. Per verificare che A è un campo consideriamo un elemento $x \neq 0$ di A. Per la regolarità esiste $y \in A$ con $x = yx^2$. Allora da $x \neq 0$ e $x(1 - xy) = 0$ deduciamo che $1 - xy = 0$ poiché A è un dominio. Allora x è invertibile e A è un campo.

(b) Sia $\pi : A \longrightarrow A/I$ l'omomorfismo canonico. Per $a \in A/I$ sia $x \in A$ tale che $\pi(x) = a$. Esiste $y \in A$ con $x = yx^2$. Allora $b = \pi(y)$ soddisfa $a = ba^2$.

(c) Sia P un ideale primo di A. Allora il quoziente A/P è un dominio. D'altra parte A/P è anche regolare per il punto (b). Allora A/P risulta un campo per il punto (a). Questo dimostra che l'ideale P è massimale.

(d) Se $I = (x)$, troviamo $y \in A$ con $x = yx^2$. Allora $e = xy$ è un idempotente e $I = (e)$.

(e) Sia $a = (a_s)_{s \in S}$ un elemento di K^S. Per il punto (a), K è regolare e quindi troviamo per ogni $s \in S$ un elemento $b_s \in K$ con $a_s = a_s^2 b_s$. Allora $b = (b_s)_{s \in S}$ soddisfa $a = a^2 b$. Pertanto K^S è regolare.

13.10 Esercizi del capitolo 10

10.1 Si consideri l'anello $A = 2\mathbb{Z}$ dei numeri interi pari. Allora B ha divisori dello zero.

10.3 (c) Basta vedere che φ_a è invertibile, notando che dal punto (b), con $b = a^{-1}$, si ricava $\varphi_a \circ \varphi_{a^{-1}} = \varphi_1 = id_A$.

10.4 Sia $\pi : A \longrightarrow A/I$ l'omomorfismo canonico. Supponiamo che I sia massimale. Allora per un ideale proprio J di A/I l'ideale proprio $\pi^{-1}(J)$ di A contiene $I = \ker \pi$. Quindi $\pi^{-1}(J) = I$. Di conseguenza $J = \pi(\pi^{-1}(J)) = \pi(I) = \overline{0}$. Questo dimostra che A/I non ha ideali propri. Per il lemma 9.22 A/I è un campo.

Adesso supponiamo che A/I sia un campo e I non sia un ideale massimale. Sia L un ideale proprio di A contenente I propriamente. Allora $\pi(L)$ è un ideale proprio di A/I, assurdo.

10.6 Sia G il gruppo abeliano $(A, +)$. Per ogni elemento $a \in A$ consideriamo l'applicazione $\mu_a : A \longrightarrow A$ definita da $\mu_a(x) = ax$. Allora μ_a è un endomorfismo di G. Inoltre per ogni $b \in A$ μ_{ab} coincide con la composizione $\mu_a \circ \mu_b$, mentre μ_{a+b}

coincide con la somma $\mu_a + \mu_b$. Pertanto il sottoinsieme $A_1 = \{\mu_a : a \in A\}$ di $End(G)$ è un sottoanello di $End(G)$. Usando l'unità di A si vede facilmente che μ_a coincide con l'endomorfismo nullo di G precisamente quando $a = 0$. Questo ci permette di identificare l'anello A con un sottoanello dell'anello $End(G)$ tramite l'omomorfismo di anelli $\varrho : A \to End(G)$ definito da $\varrho(a) = \mu_a$.

10.9 Siano $G = \mathbb{Z}^{\mathbb{N}}$ e $f : G \to G$ definito da

$$f(x_1, x_2, x_3, \ldots) = (0, x_1, x_2, x_3, \ldots).$$

Allora f è un endomorfismo iniettivo e pertanto per l'esercizio 10.8 f non è suriettivo. D'altro canto se si considera $g : G \to G$ definito da

$$g(x_1, x_2, x_3, \ldots) = (x_1, 0, 0, 0, \ldots),$$

si ha $g \neq 0$ ma $g \circ f = 0$ in $\mathrm{End}(G)$.

10.11 Provare che l'assegnazione

$$q = a + bi + cj + dk \mapsto \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

risulta un isomorfismo $\mathbb{H} \to B$.

10.12 (a) Sia $\phi : \mathbb{Z} \to \mathbb{Z}$ omomorfismo di anelli; allora con $n = \phi(1)$ si ha

$$\phi(x) = nx \text{ per ogni } x \in \mathbb{Z}.$$

Inoltre

$$n = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = n \cdot n = n^2.$$

Le uniche soluzioni di $n = n^2$ in $\mathbb{Z}$ sono $n = 0$ oppure $n = 1$. Nel primo caso, $\phi(x) = 0$ per ogni $x \in \mathbb{Z}$, cioè ϕ è l'omomorfismo nullo; nell'altro caso, $\phi(x) = x$ per ogni $x \in \mathbb{Z}$, ossia ϕ è l'identità su $\mathbb{Z}$. Pertanto l'unico endomorfismo di anelli unitari di $\mathbb{Z}$ è l'identità di $\mathbb{Z}$.

Nel seguito consideriamo solamente omomorfismi di anelli unitari.

(b) Per individuare gli endomorfismi $\phi : \mathbb{Q} \to \mathbb{Q}$, osserviamo che $\phi(1) = 1$. Se $\frac{1}{n} \in \mathbb{Q}$, allora

$$n \cdot \frac{1}{n} = 1, \quad \text{e} \quad 1 = \phi(1) = \phi\left(\frac{1}{n}\right)\phi(n),$$

quindi

$$\phi\left(\frac{1}{n}\right) = \frac{1}{\phi(n)} = \frac{1}{n}.$$

Allora per ogni $\frac{r}{s} \in \mathbb{Q}$,

$$\phi\left(\frac{r}{s}\right) = \phi\left(r \cdot \frac{1}{s}\right) = \phi(r)\phi\left(\frac{1}{s}\right) = r \cdot \frac{1}{s} = \frac{r}{s};$$

pertanto ϕ è l'identità su $\mathbb{Q}$.

(c) Si osservi che se $\phi : \mathbb{R} \to \mathbb{R}$ è omomorfismo di anelli unitari, allora per il punto (b) ϕ è identico su $\mathbb{Q}$. Inoltre ogni $x > 0$ si può scrivere come $x = z^2$, quindi anche $\phi(x) = \phi(z)^2 > 0$. Possiamo concludere che ϕ conserva l'ordine:

$$x \geq y \Rightarrow \phi(x) \geq \phi(y).$$

Per l'osservazione 10.11 $\ker \phi = 0$, cioè ϕ è iniettiva. Ora supponiamo per assurdo di avere $x \in \mathbb{R}$ con $\phi(x) \neq x$. Consideriamo il caso in cui $x < \phi(x)$. Per la densità di $\mathbb{Q}$ in $\mathbb{R}$ esiste $r \in \mathbb{Q}$ con $x < r < \phi(x)$. Per ciò che abbiamo detto prima $\phi(x) < \phi(r) = r$, assurdo. Si ragiona analogamente nel caso in cui $x > \phi(x)$. Abbiamo dimostrato che ϕ è identica anche su $\mathbb{R}$.

(d) Poiché $i^2 = -1$, necessariamente $\phi(i) = \pm i$ per ogni omomorfismo di anelli unitari $\mathbb{Z}[i] \to \mathbb{Z}[i]$. Il resto segue da (a).

(e) Per $\phi : \mathbb{Z}[\sqrt{n}] \to \mathbb{Z}[\sqrt{n}]$, ϕ è l'identità su $\mathbb{Z}$ e

$$[\phi(\sqrt{n})]^2 = \phi(\sqrt{n})(\phi\sqrt{n}) = \phi(n) = n,$$

pertanto $\phi(\sqrt{n}) = \pm\sqrt{n}$: gli unici omomorfismi $\mathbb{Z}[\sqrt{n}] \to \mathbb{Z}[\sqrt{n}]$ sono

l'identità $x + \sqrt{n}y \mapsto x + \sqrt{n}y$ e la coniugazione $x + \sqrt{n}y \mapsto x - \sqrt{n}y$.

10.18 (a) Prendere $I_1 = (1,0)I$ e $I_2 = (0,1)I$.

(c) Se $I_1 \neq A$ e $I_2 \neq B$, si consideri $x \in A \setminus I_1$ e $y \in B \setminus I_2$. Ora $(x,0)(0,y) = (0,0) \in I$, ma $(x,0) \notin I$ e $(0,y) \notin I$.

(d) $C/I \cong A/I_1$ è un dominio.

(f) $C/I \cong A/I_1$ è un campo.

(g) Applicare (a).

10.21 Ragioniamo per induzione su n. Per il caso $n = 2$, sia $I = I_1 \cap I_2$ e applichiamo il teorema 10.20 all'anello A/I e ai suoi ideali I_1/I e I_2/I. Se $n > 2$, denotando con

$$I = \bigcap_{k=1}^{n-1} I_k$$

abbiamo

$$A/I \cong A/I_1 \times A/I_2 \times \ldots \times A/I_{n-1}$$

per l'ipotesi induttiva. D'altra parte, usando l'esercizio 9.30 abbiamo $I + I_n = A$. Quindi

$$A/(I \cap I_n) \cong A/I \times A/I_n \cong A/I_1 \times A/I_2 \times \ldots \times A/I_n.$$

10.22 Basta applicare l'esercizio 10.21 e l'esercizio 9.30.

10.23 Sia A un anello commutativo unitario finito e siano $M_1, M_2, \ldots, M_s$ i suoi ideali massimali. Per l'esercizio 9.31 esiste $k \in \mathbb{N}_+$ tale che $\bigcap_{i=1}^{s} M_i^k = \{0\}$. Applicando l'esercizio 10.22 si ricava

$$A \cong \prod_{j=1}^{s} A/M_j^k.$$

Ora basta notare che A/M_j^k è locale per il punto (b) dell'esercizio 9.30.

10.24 (a) Si verifica immediatamente che l'omomorfismo $\iota_R : R \to R[G]$ risulta omomorfismo di anelli unitari quando R è unitario.

10.25 Usando il punto (d) dell'esercizio 10.24, applicato a G_1 visto come sottogruppo di $G_1 \times G_2$ nel modo usuale, troviamo un omomorfismo di anelli unitari iniettivo $\rho : R[G_1] \to R[G_1 \times G_2]$. Ora applicando il punto (c) dell'esercizio 10.24 all'omomorfismo ρ e all'omomorfismo $h : G_2 \to R[G_1 \times G_2]$ definito da $h(g) = 1_R(e_{G_1}, g)$, si trova un omomorfismo di anelli unitari

$$f : (R[G_1])[G_2] \to R[G_1 \times G_2].$$

Per vedere che f è suriettiva, si prenda una coppia $(g_1, g_2) \in G_1 \times G_2$ e si consideri il prodotto $g_1 g_2 \in (R[G_1])[G_2]$, dove g_1 è considerato come elemento di $R[G_1]$. Si verifichi che $f(g_1 g_2) = (g_1, g_2)$. Questo permette di verificare che f è suriettiva. Si dimostra che f è iniettiva, per l'esercizio 10.24.

10.26 Abbiamo visto nell'esercizio 9.20 che $I_1 = (g-1)$ e $I_2 = (g+1)$ sono ideali massimali di $A = \mathbb{R}[G]$ con $A/I_1 \cong A/I_2 \cong \mathbb{R}$, dove g è il generatore di G. Essendo $I_1 I_2 = I_1 \cap I_2 = \{0\}$, concludiamo per l'esercizio 10.22 che

$$A \cong A/I_1 \times A/I_2 \cong \mathbb{R} \times \mathbb{R}.$$

10.27 Sia g il generatore di G. Allora $I_1 = (g-1)$ e $I_2 = (g^2 + g + 1)$ sono ideali massimali di $A = \mathbb{R}[G]$ e $A/I_1 \cong \mathbb{R}$. Per verificare che $A/I_2 \cong \mathbb{C}$ basta fissare una delle due radici terze dell'unità complesse ξ e definire un omomorfismo suriettivo

$$f : A \to \mathbb{C} \quad \text{con} \quad f(r_0 + r_1 g + r_2 g^2) = r_0 + r_1 \xi + r_2 \xi^2.$$

Essendo $\ker f = I_2$ ricaviamo un isomorfismo $f : A/I_2 \cong \mathbb{C}$. Ora da $I_1 I_2 = I_1 \cap I_2 = \{0\}$, concludiamo per l'esercizio 10.22 che

$$A \cong A/I_1 \times A/I_2 \cong \mathbb{R} \times \mathbb{C}.$$

10.29 Sia $(G, \cdot)$ il gruppo ciclico di ordine 2 e sia a un suo generatore. Allora $a^2 = 1$ in $R[G]$. Pertanto $j = \frac{a+1}{2}$ è un idempotente di $R[G]$ e l'ideale principale (j) di $R[G]$ è isomorfo a R come anello unitario tramite l'isomorfismo $r \mapsto rj$. Analogamente $(1-j) \cong R$ come anelli unitari. Per l'esercizio 10.21

$$R[G] \cong (j) \times (1-j) \cong R \times R.$$

10.31 Sia a il generatore del gruppo G. Supponiamo di avere un idempotente $j \in R[G]$ diverso da 0 e 1. Esistono $r, s \in R$ tali che $j = r + sa$. Allora

$$j^2 = (r^2 + s^2) + 2rsa = r + sa = j$$

e quindi $2rs = s$. Se s fosse 0, dall'uguaglianza $r^2 + s^2 = r$ ricaviamo $r^2 = r$ e $j = r = 0$ o 1, assurdo. Quindi $s \neq 0$ e pertanto $2r = 1$, poiché R è un dominio. Questo dimostra che 2 è invertibile in R.

10.32 Segue immediatamente dagli esercizi 10.29 e 10.31.

10.33 (a) Se $b \in B$ si ha

$$b + 1 = (b + 1)^2 = b^2 + 2b + 1 = b + 2b + 1.$$

Di conseguenza $2b = 0$ per ogni $b \in B$.

(b) Se B fosse dominio di integrità, per ogni $b \in B$ avremmo $0 = b^2 - b = b(b-1)$, quindi $b = 0$ o $b = 1$. Di conseguenza, $B = \{0, 1\} = \mathbb{Z}_2$.

(c) Se P è un ideale primo di B, allora il quoziente è un dominio tale che $\overline{b} = \overline{b}^2$ vale per ogni elemento. Questo significa che $B/P \cong \{0, 1\} = \mathbb{Z}_2$ è un campo. Pertanto P è un ideale massimale. Una soluzione alternativa è di notare che ogni anello di Boole è regolare e applicare (c) dell'esercizio 9.51.

(d) Basta dimostrare che ogni ideale del tipo $I = (a) + (b)$ è principale. Ovviamente l'elemento $c = a + b + ab$ di I soddisfa $ca = a$ e $cb = b$. Quindi (c) contiene sia a che b e di conseguenza I. Questo dimostra $I = (c)$.

(e) Se B è finito, allora, essendo spazio vettoriale sul suo sottoanello fondamentale $B_0 = \{0, 1\} \cong \mathbb{Z}_2$, risulta $B \cong \mathbb{Z}_2^n$ per un opportuno n, ove l'isomorfismo è un morfismo di spazi vettoriali sul campo $\mathbb{Z}_2$. Pertanto $|B| = 2^n$. Per dimostrare che $B \cong \mathbb{Z}_2^n$ come *anelli*, ragioniamo per induzione su n. Per $n = 1$ l'asserto è ovvio. Supponiamo che sia vero per tutti gli anelli Booleani B con $|B| < 2^n$ e con $n > 1$. Poiché $|B| = 2^n > 2$, esiste $b \in B$, $b \neq 0, 1$. Allora $b^2 = b$, e quindi $b(b-1) = 0$. Gli ideali principali $R_1 = (b)$ e $R_2 = (b-1)$ sono anelli di Boole di cardinalità $< 2^n$. Per l'ipotesi induttiva $R_1 \cong \mathbb{Z}_2^k$ e $R_2 \cong \mathbb{Z}_2^m$ come anelli unitari. Per l'esercizio 10.28, si ha

$$B \cong R_1 \times R_2 \quad \text{e quindi} \quad B \cong \mathbb{Z}_2^n.$$

10.35 Con l'ordine definito dall'inclusione $\mathcal{P}(X)$ risulta un reticolo distributivo e limitato. Ora basta notare che, per ogni $A \in \mathcal{P}(X)$, il complemento di A è l'usuale complemento $X \setminus A$ di A in X.

10.36 Verificare che l'insieme ordinato $(\mathcal{I}(L), \leq)$ è induttivo e applicare il lemma di Zorn.

10.38 $\{1, 2, 4\}$, $\{1, 2, 3, 4, 6, 12\}$, $\{1, 3, 9\}$ e $\{1, 2, 3, 6, 9, 18\}$.

10.39 Verificare che l'insieme ordinato $(F(X), \leq)$ è induttivo e applicare il lemma di Zorn.

10.42 (f) Per $Y \subsetneq X$ denotiamo con i_Y l'unico idempotente di A con $Z(i_Y) = Y$. Allora per ogni $f \in A$ si ha $(f) = (i_{Z(f)})$.

(g) Basta notare che per $f, g \in A$ si ha $(f) + (g) = (i_{Z(f) \cap Z(g)})$ e poi procedere per induzione sul numero dei generatori dell'ideale.

(h) Sia I un ideale primo di A e $f \notin I$ un elemento di A. Allora $(f) \not\subseteq I$ e per il punto (f) non è restrittivo assumere che f sia idempotente, cioè $f^2 - f = 0$. Ora $f(1 - f) = 0 \in I$, $f \notin I$ e I è primo, dunque $1 - f \in I$. Si conclude

$$1 = f + (1 - f) \in (f) + I, \quad \text{quindi} \ (f) + I = A.$$

(i) $M_x = (i_{\{x\}})$.

(j) $A/M_x \cong K$ è un campo.

(k) Sia I un ideale massimale finitamente generato. Allora $I = (i_Y)$ per (g), in più $Y = \{x\}$ per un opportuno $x \in X$, poiché I è massimale. Quindi $I = M_x$.

(l) Con $X = \mathbb{N}$ o qualsiasi insieme infinito si consideri l'insieme I delle funzioni $f \in A$ tali che $X \setminus Z(f)$ è finito. Provare che I è un ideale proprio di A. Per il lemma di Krull 9.33, esiste un ideale massimale M di A che contiene I. Poiché $I \not\subseteq M_x$ per ogni $x \in X$, $M \neq M_x$ per ogni $x \in X$.

(m) Se $\phi : X \to Y$ è una biezione, l'applicazione $\Phi : K^Y \to K^X$ definita da $\Phi(h) = h \circ \phi$ per $h \in K^Y$ è un isomorfismo.

(n) Per $i = 1, 2$ definire l'idempotente $e_i \in A$ con $X \setminus X_i = Z(e_i)$. Chiaramente

$$e_1 + e_2 = 1, \quad e_1 e_2 = 0 \quad \text{e} \quad (e_1) \cong K^{X_1}, \quad (e_2) \cong K^{X_2}.$$

Poiché $A \cong (e_1) \times (e_2)$, abbiamo

$$A \cong K^{X_1} \times K^{X_2}.$$

(o) Applicare (m) e (n) con $X = \mathbb{N}$ o qualsiasi insieme infinito.

(p*) Per $I \lhd A$ considerare la famiglia $\mathcal{F}_I = \{Z(f) : f \in I\}$, per un filtro $\mathcal{F}$ considerare l'ideale $I_{\mathcal{F}}$ generato dalle funzioni i_F con $F \in \mathcal{F}$.

10.43 Ragionare come nell'esercizio 10.42.

10.46 Sia $\alpha = x + \sqrt{5}y \in A$; allora

$$\alpha \in M \iff N(\alpha) \equiv_2 0 \iff$$

$$x^2 - 5y^2 \equiv_2 x^2 + y^2 \equiv_2 (x + y)^2 \equiv_2 x + y \equiv_2 0 \iff x \equiv_2 y.$$

Si verifica direttamente che M è un ideale. Oppure: si consideri l'applicazione $\phi : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}_2$, $x + \sqrt{5}y \mapsto x + y + 2\mathbb{Z}$. Verificare che ϕ è omomorfismo suriettivo e $\ker \phi = \{x + \sqrt{5}y \in A : x + y \equiv 0 \pmod 2\} = M$. Poiché $\mathbb{Z}_2 \cong \mathbb{Z}[\sqrt{5}]/M$ e $\mathbb{Z}_2$ è un campo, anche $\mathbb{Z}[\sqrt{5}]/M$ è un campo, pertanto M è ideale massimale.

10.47 Vediamo innanzitutto che un anello regolare A ha $N(A) = \{0\}$. Infatti se $a \in N(A)$, allora ogni elemento di $I = (a)$ sarà nilpotente. Poiché I è generato da un idempotente, questo è possibile solo se $I = \{0\}$. Per ogni sottoanello B di A abbiamo $N(B) = N(A) \cap B = \{0\}$.

Supponiamo ora $N(A) = \{0\}$. Per ogni ideale primo P di A sia $f_P : A \to A/P$ l'omomorfismo canonico. Componendo f_P con l'inclusione di A/P nel suo campo

di quozienti $Q(A/P)$ troviamo un omomorfismo $g_P : A \to Q(A/P)$ con nucleo $\ker g_P = P$ nel campo $Q(A/P)$. La famiglia di omomorfismi

$$\{g_P : P \text{ ideale primo di } A\}$$

dà luogo ad un omomorfismo

$$g : A \to R = \prod_P Q(A/P)$$

con nucleo

$$\bigcap_P \ker g_P = \bigcap P = N(A) = \{0\}$$

per l'esercizio 9.24. L'anello R risulta regolare in quanto prodotto di anelli regolari per l'esercizio 9.51. Abbiamo dimostrato che ogni anello commutativo A con $N(A) = \{0\}$ è isomorfo ad un sottoanello di un anello regolare.

13.11 Esercizi del capitolo 11

11.2 Sia $f(x) = a_0 + a_1x + \ldots + a_nx^n \in A[x]$. Chiaramente $f(x)$ è nilpotente se tutti i coefficienti a_i sono nilpotenti. Infatti somma di elementi nilpotenti è nilpotente. Supponiamo ora che $(f(x))^k = 0$. Per dimostrare che tutti i coefficienti a_i sono nilpotenti ragioniamo per induzione su n. Il caso $n = 0$ è banale. Supponiamo $n > 0$ e l'asserto vero per $n - 1$. Poniamo $h(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ e notiamo che $f(x) = h(x) + a_nx^n$. Inoltre il coefficiente direttivo di $(f(x))^k$ è a_n^k. Quindi $(f(x))^k = 0$ implica $a_n^k = 0$. Dunque il polinomio a_nx^n è nilpotente. Allora anche $h(x) = f(x) - a_nx^n$ è nilpotente ed è di grado $n - 1$. Per l'ipotesi induttiva tutti coefficienti a_i per $i = 0, 1, \ldots, n - 1$ sono nilpotenti.

11.3 Sia $g(x) + I$ un elemento arbitrario di $A[x]/I$. Per l'algoritmo della divisione in $A[x]$, esistono polinomi $q(x), r(x)$ tali che $g(x) = q(x)f(x) + r(x)$ e $\deg r < n$, qualora $r(x) \neq 0$. Poiché $q(x)f(x) \in I$ si ha $g(x) + I = r(x) + I$. D'altra parte, se $r(x), r'(x)$ sono polinomi di grado $< n$, allora $r(x) + I = r'(x) + I$ se e solo se $r(x) = r'(x)$, poiché $f(x)$ divide $(r(x) - r'(x))$ se e e solo se $r(x) - r'(x) = 0$, essendo questa differenza di grado $< n$.

11.8 Sia $a = bc$ e supponiamo che a non divida b. Allora $b = qa + r$ con $r \neq 0$ e quindi $\delta(r) < \delta(a) = \delta(b)$. Ma

$$r = b - qa = b - qbc = b(1 - qc).$$

Quindi $\delta(r) \geq \delta(b)$, assurdo.

11.10 Poiché per ogni $n \in \mathbb{N}$ ci sono un numero finito di polinomi di grado minore o uguale ad n, si può applicare l'esercizio 11.9.

11.11 Se esistono $a, b \in \mathbb{Z}$ tali che $n = a^2 + b^2$, allora $n = (a + bi)(a - bi)$.

11.12 (a) Per il teorema 11.40 per i numeri primi del tipo $p = 4k + 1$ esistono $a, b \in \mathbb{Z}$ tali che $p = a^2 + b^2$. Supponiamo ora che $p = 4k + 3$ e $a^2 + b^2 = p$. Allora

$$a^2 \equiv_p -b^2, \qquad (*)$$

essendo entrambi a, b ovviamente coprimi con p. Per il teorema di Fermat, si ha

$$a^{p-1} \equiv_p b^{p-1} \equiv_p 1.$$

D'altra parte, elevando (*) alla $2k + 1 = \frac{p-1}{2}$, abbiamo

$$1 \equiv_p a^{p-1} \equiv_p -b^{p-1} \equiv_p -1$$

(si noti che $2k + 1$ è dispari), e quindi $1 \equiv_p -1$, assurdo.

(b) Se il primo p non è del tipo $p = 4k+3$ l'asserto segue dal punto (a), l'esercizio 11.11 e dal fatto che $2 = 1^2 + 1^2$.

Supponiamo $p = 4k + 3$. Sia $p = z \cdot z_1$ in $\mathbb{Z}[i]$. Se $z = a + bi$, abbiamo allora $\delta(p) = \delta(z) \cdot \delta(z_1)$ e $\delta(z) = a^2 + b^2$. Quindi $a^2 + b^2$ divide $p^2 = \delta(p)$. Dal punto (a) segue che $a^2 + b^2 \neq p$. Quindi restano due possibilità $a^2 + b^2 = 1$ oppure $a^2 + b^2 = p^2$. Nel primo caso $\delta(z) = 1$, e quindi z è invertibile, nel secondo caso $\delta(z_1) = 1$, e quindi z_1 è invertibile.

11.14 Si ha $2 = (1+i)(1-i), 5 = (2+i)(2-i), 17 = (4+i)(4-i), 6-3 = 3(2i-1)$, dove $2i - 1$ e $1 + 2i$ sono primi avendo norma $1^2 + 2^2 = 5$.

11.17 Sia a un generatore di I e sia $a = p_1^{k_1} \dots p_s^{k_s}$ una fattorizzazione di a con p_i elementi irriducibili e due a due non associati. Un elemento del tipo $x = b + I$ di B è non invertibile precisamente quando x è contenuto in qualche ideale massimale M di B. Poiché tale M deve essere della forma $M = J/I$, dove J è un ideale massimale di A contenente I, ricaviamo che $J = (p_i)$ per qualche $i = 1, 2, \dots, s$. In altre parole, $x = b + I$ è non invertibile precisamente quando $b \in (p_i)$ (cioè $p_i | b$) per qualche $i = 1, 2, \dots, s$. Definiamo ora

$$c = p_1^{k_1} \dots p_{i-1}^{k_{i-1}} p_i^{k_i - 1} p_{i+1}^{k_{i+1}} \dots p_s^{k_s}.$$

Chiaramente $c \notin I$, quindi $y = c + I \neq 0$ in B. D'altra parte $bc \in I$, e quindi $yx = 0$ in B. Pertanto x è divisore dello zero.

11.18 Se $I = (p^n)$ con $n \geq 1$, allora da $ab \in I$ e $a \notin I$ deduciamo che p^n divide ab ma non divide a. Quindi $p|b$, da cui p^n divide b^n, cioè $b^n \in I$.

11.20 Applicare il criterio di Eisenstein.

11.21 Applicare il criterio di Eisenstein per $p = 3$.

11.22 Supponiamo I principale, cioè $I = (f)$ per qualche $f \in \mathbb{Z}[x]$. Allora $2 \in I$, quindi $2 = fg$ per qualche $g \in \mathbb{Z}[x]$. Poiché il polinomio costante 2 ha grado 0, deve essere $\deg f = 0$ e quindi $f = a \in 2\mathbb{Z}$. Inoltre $x \in I$, pertanto $x = ag$ per qualche

$g \in \mathbb{Z}[x]$, con $g = b_0 + b_1 x$. Si ottiene $b_1 a = 1$ e questo è impossibile. Quindi I non è principale.

11.24 Considerare la riduzione modulo 2. Il polinomio

$$f(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$$

è irriducibile. Infatti non è difficile vedere che $x^2 + x + 1$ è l'unico polinomio irriducibile di grado 2 in $\mathbb{F}_2[x]$. Quindi, non avendo radici in $\mathbb{F}_2$, il polinomio $f(x)$ potrebbe essere riducibile solo se fosse divisibile per $x^2 + x + 1$. Ma

$$f(x) = (x^2 + x + 1)^2 + x^3 + x^2,$$

quindi $x^2 + x + 1$ divide $f(x)$ se e solo se divide $x^3 + x^2 = x(x^2 + 1)$. Essendo irriducibile, $x^2 + x + 1$ non divide $x(x^2 + 1)$, poiché non divide $x^2 + 1$.

11.25 Considerare la riduzione modulo 2.

11.26 Sia M un ideale massimale di $\mathbb{Z}[x]$. Dimostriamo che M non può essere principale. Supponiamo $M = (f(x))$. Essendo M massimale, M è anche un ideale primo, quindi $f(x)$ deve essere irriducibile per i lemmi 11.27 e 11.29. Se $f(x) = p$ è di grado 0, allora M non è massimale in quanto $M + (x)$ è ancora un ideale proprio che contiene M propriamente. Quindi $\deg f = n > 0$. Sia a_n il coefficiente direttivo di $f(x)$ e sia p un primo tale che p non divide a_n. Allora $p \notin M = (f(x))$ e pertanto $(p) + (f(x)) = \mathbb{Z}[x]$. Quindi esistono $h(x) \in \mathbb{Z}[x]$ e $g(x) \in \mathbb{Z}[x]$, con $ph(x) + f(x)g(x) = 1$. Passando all'anello quoziente

$$\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x]$$

si ha

$$\overline{f(x)} \cdot \overline{g(x)} = 1.$$

Ma per la scelta di p, si ha $\deg \overline{f} = n > 0$, assurdo. Questo mostra che M non è principale.

11.27 Sia M un ideale massimale di $\mathbb{Z}[x]$ e sia $f(x) \in M$ un polinomio irriducibile. Sappiamo che M non può essere principale per l'esercizio 11.26. Allora $M \neq (f(x))$, quindi possiamo trovare $g(x) \in M$ con $g(x) \notin (f(x))$. Dunque $f(x)$ non divide $g(x)$ nell'anello $\mathbb{Z}[x]$. Poiché $f(x)$ è primitivo, $f(x)$ non divide $g(x)$ neanche nell'anello $\mathbb{Q}[x]$. Il polinomio $f(x)$ essendo irriducibile in $\mathbb{Z}[x]$, risulta irriducibile anche come elemento dell'anello $\mathbb{Q}[x]$, quindi genera un ideale massimale, in quanto $\mathbb{Q}[x]$ è un dominio principale. Ora dal fatto che $f(x)$ non divide $g(x)$ in $\mathbb{Q}[x]$, concludiamo che questi due polinomi sono coprimi in $\mathbb{Q}[x]$ e pertanto esistono $u(x), v(x) \in \mathbb{Q}[x]$, con $u(x)f(x) + v(x)g(x) = 1$. Scegliamo un intero m tale che $u_1 = mu(x) \in \mathbb{Z}[x]$ e $v_1 = mv(x) \in \mathbb{Z}[x]$. Allora

$$u_1(x)f(x) + v_1(x)g(x) = m \in \mathbb{Z} \cap M.$$

Quindi $\mathbb{Z} \cap M$ è un ideale non nullo di $\mathbb{Z}$. Per il teorema di corrispondenza 10.6 $\mathbb{Z} \cap M$ è un ideale massimale e quindi anche primo di $\mathbb{Z}$. Quindi esiste un numero

primo p con $\mathbb{Z} \cap M = p\mathbb{Z}$. Sia $I = p\mathbb{Z}[x]$, allora M contiene l'ideale I di $\mathbb{Z}[x]$ e per il teorema 10.6 M/I è un ideale massimale di $\mathbb{Z}[x]/I \cong \mathbb{F}_p[x]$. Per l'esercizio 11.10 ogni ideale non nullo di $\mathbb{F}_p[x]$ ha indice finito ed essendo

$$\mathbb{Z}[x]/M \cong \mathbb{F}_p[x]/(M/I),$$

concludiamo che M ha indice finito in $\mathbb{Z}[x]$.

Per quanto riguarda l'anello $\mathbb{Q}[x]$ basta notare che per ogni ideale massimale M di $\mathbb{Q}[x]$ l'intersezione $\mathbb{Q} \cap M$ è un ideale proprio di $\mathbb{Q}$. Quindi $\mathbb{Q} \cap M = \{0\}$. Questo significa che il quoziente $\mathbb{Q}[x]/M$ contiene una copia di $\mathbb{Q}$ e quindi è infinito.

11.28 Sia M un ideale massimale di $\mathbb{Z}[x]$. Per lo svolgimento dell'esercizio 11.27 esiste un numero primo p con $\mathbb{Z} \cap M = p\mathbb{Z}$. In particolare $p \in M$ e pertanto il nucleo (p) dell'omomorfismo canonico $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ è contenuto in M, quindi $N = \varphi(M)$ è un ideale massimale di $\mathbb{Z}_p[x]$. Allora esiste un polinomio $\overline{f(x)}$ irriducibile su $\mathbb{Z}_p$, tale che $N = (\overline{f(x)})$ e pertanto $M = \varphi^{-1}(N) = (p, f(x))$, con $f(x) \in \mathbb{Z}[x]$ tale che $\varphi(f(x)) = \overline{f(x)}$.

Non è difficile dimostrare che se p è un primo e se $f(x) \in \mathbb{Z}[x]$ è tale che $\overline{f(x)}$ risulta irriducibile su $\mathbb{Z}_p$, allora $M = (p, f(x))$ è un ideale massimale di $\mathbb{Z}[x]$. Infatti M contiene il nucleo (p) dell'omomorfismo canonico φ, quindi M è massimale se e solo se $N = \varphi(M)$ è massimale. Ma $N = (\overline{f(x)})$ è massimale per l'ipotesi su $\overline{f(x)}$.

11.29 $f(x) = (x^3 - 2x)(x^2 + 1) + (2x + 1)$ e si vede facilmente che $(x^2 + 1)$ e $(2x + 1)$ sono coprimi. Di conseguenza, anche $f(x)$ e $g(x)$ sono coprimi.

11.31 Il polinomio $f(x)$ è irriducibile in $\mathbb{Z}_5[x]$ perché non ha radici. Allora $\mathbb{Z}_5[x]/(f)$ è un campo e i suoi elementi sono $h + (f)$ con $h \in \mathbb{Z}_5[x]$. Dalla divisione euclidea: $h = fq + r$, essendo $\deg r < 3$, riducendo modulo f si ottiene $\deg h < 3$. Allora $h(x) = a_0 + a_1 x + a_2 x^2$ e possiamo scegliere i coefficienti $a_i \in \mathbb{Z}_5$ in $5^3 = 125$ modi. Quindi $\mathbb{Z}_5[x]/(f)$ è un campo con 125 elementi. Per ricavarne uno con 25 elementi, si consideri il polinomio $g(x) = x^2 + 2$.

11.32 L'anello A non è campo: $x^2 - 2 + I$ è un elemento nilpotente non nullo. Osserviamo che

$$h + I \in A \ \text{ è invertibile } \iff (h, f) = 1.$$

Pertanto $x + 1 + I$ è invertibile e l'inverso si determina con il procedimento di divisione euclidea:

$$1 = f(x) + (x + 1)(-x^3 + x^2 + 3x - 3)$$

e, riducendo modulo I, si ottiene che l'inverso di $x + 1 + I$ è

$$-x^3 + x^2 + 3x - 3 + I.$$

Si ha inoltre

$h(x) + I$ è non invertibile $\iff$ h ed f non sono coprimi $\iff$ $x^2 - 2$ divide $h(x)$.

Allora

$$M = \{h + I : h \in (x^2 - 2)\} = (x^2 - 2)/(f).$$

Essendo $x^2 - 2$ irriducibile in $\mathbb{Q}[x]$ si ha

$$\frac{\mathbb{Q}[x]}{(x^2-2)} \cong \frac{\mathbb{Q}[x]/(f)}{(x^2-2)/(f)} \cong \frac{A}{M},$$

A/M è campo e quindi M è ideale massimale di A.

11.34 Sia $h(x) = 1 + x + \ldots + x^{p-1}$. Poiché $x^p - 1 = (x-1)h(x)$ e $h(x)$ è irriducibile, si veda l'esempio 11.59, la fattorizzazione richiesta è

$$x^p - 1 = (x-1)h(x).$$

11.35 Si ha

$$f(x) = x^4 + 3 = x^4 - 4 = (x^2+2)(x-3)(x+3).$$

Per (a) basta notare che $x^2 + 1$ è coprimo con $f(x)$. Per (b) si noti che $g(x) = x^2 - 4x + 3 = (x-1)(x-3)$, da cui segue che

$$(g(x) + I)(x^2+2)(x+3) + I = 0 + I \quad \text{e} \quad g(x) + I \neq 0.$$

Otteniamo così due divisori dello zero in A. Se $J = (d(x))$ contiene l'ideale $I = (f(x))$, allora $d(x)$ divide $f(x)$. Inoltre se $g(x) \in J$, allora $d(x)$ divide $g(x)$, quindi $d(x)$ divide il massimo comun divisore $x - 3$ di $f(x)$ e $g(x)$.

11.36 Ci riduciamo modulo 2, allora $\overline{f}(x) = x^4 + x + 1$. Questo polinomio non ha radici in $\mathbb{Z}_2$, quindi non può avere fattori di primo grado. L'unico polinomio di secondo grado che non ha radici in $\mathbb{Z}_2$ è x^2+x+1. Quindi la possibile fattorizzazione di f dovrebbe essere: $\overline{f}(x) = (x^2+x+1)^2$, ma questo è falso. Quindi $\overline{f}$ irriducibile in $\mathbb{Z}_2[x] \Rightarrow f$ irriducibile in $\mathbb{Q}[x]$.

Supponiamo per assurdo che $g(x)$ sia riducibile. In tal caso $g(x) = h(x)q(x)$, dove $h(x)$ e $q(x)$ sono polinomi monici in $\mathbb{Z}[x]$, essendo $g(x)$ un polinomio monico. Inoltre deve essere $\deg h = \deg q = 2$, non avendo $g(x)$ radici in $\mathbb{Q}$. Proiettando in $\mathbb{Z}_2[x]$ troviamo una decomposizione $\overline{g(x)} = \overline{h(x)}\ \overline{q(x)}$ in prodotto di due polinomi di secondo grado in $\mathbb{Z}_2[x]$. D'altra parte $\overline{g(x)} = x(x^3 + x^2 + 1)$ e il polinomio $(x^3 + x^2 + 1)$ è irriducibile in $\mathbb{Z}_2[x]$. Pertanto l'uguaglianza

$$\overline{h(x)}\ \overline{q(x)} = x(x^3 + x^2 + 1)$$

contraddice il fatto che $\mathbb{Z}_2[x]$ è un dominio fattoriale. Questa contraddizione dimostra che $g(x)$ è irriducibile.

11.37 Il polinomio $f(x)$ si fattorizza in $K = \mathbb{Z}_3$,

$$f(x) = (x+1)^2(x^2 - x - 1).$$

L'elemento $h + (f) \in K/(f)$ è nilpotente se e solo se

$$h \text{ è multiplo di } (x+1)(x^2-x-1);$$

quindi l'insieme degli elementi nilpotenti di $K/(f)$ è l'ideale

$$((x+1)(x^2-x-1))/(f).$$

Per provare che $x^2+1+(f)$ è invertibile, dividiamo $f(x)$ per x^2+1 con l'algoritmo di Euclide e otteniamo

$$1 \equiv (x^2+1)(-1+(x-1)(x^2+x)) \ mod(f),$$

quindi l'inverso di $x^2+1+(f)$ è $x^3-x-1+(f)$. Osserviamo infine che I è ideale di A se e solo se I è del tipo $(g+(f))$, con g divisore di f. Gli ideali di A sono quindi:

$$A, \quad 0, \quad ((x+1)+(f)), \quad ((x+1)^2+(f)),$$
$$((x^2-x-1)+(f)), \quad ((x+1)(x^2-x-1))+(f)).$$

11.38 Si ha $(x^2+x+1)^2 \in J$, ma $x^2+x+1 \notin J$. Quindi J non è primo e tantomeno massimale. L'ideale I è massimale, si veda lo svolgimento dell'esercizio 11.28 e quindi è anche primo.

In $\mathbb{F}_7$ si ha $f(x) = (x^2-4)(x^2-2) = (x+2)(x-2)(x+3)(x-3)$.

11.39 Sia $A = \mathbb{Q}[y]$. Allora $f(x) = x^2 - y^3 \in A[x]$ è un polinomio primitivo. Supponiamo che $f(x)$ non sia irriducibile. Allora

$$f(x) = (x+g(y))(x+h(y)),$$

con $g(y), h(y) \in A$. È facile vedere che $h(y) = -g(y)$ e $(g(y))^2 = y^3$, assurdo. Quindi $f(x)$ è irriducibile.

11.40 Ragioniamo per assurdo come nello svolgimento dell'esercizio 11.39. Allora, essendo $f(x,y) = x^2+y^2-1$ monico, esisterebbero $g(y), h(y) \in A$ con

$$f(x,y) = (x+g(y))(x+h(y)).$$

Chiaramente $h(y) = -g(y)$. Questo implica $(g(y))^2 = y^2 - 1$, assurdo.

11.41 Non è difficile vedere che $(x-y)(x+y+1) \in I$, mentre $x - y \notin I$ e $x+y+1 \notin I$. Pertanto I non è primo. Provare che gli ideali

$$M_1 = (x^2+x+1, x-y) \quad \text{ed} \quad M_2 = (x^2+x+1, x+y+1)$$

sono massimali e $I = M_1 \cap M_2$.

11.43 (a) Se $I = (a)$, allora $I^2 = (a^2)$ e quindi $a \notin I^2$. Infatti, se $a \in I^2$, esisterebbe $b \in A$ con $a = ba^2$ e allora $a(1-ab) = 0$, assurdo perché a non è né divisore dello 0 né invertibile.

(b) Sia $I = (a)$. Allora $a \neq 0$ è un elemento non invertibile, quindi si fattorizza in prodotto di elementi irriducibili $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, dove $p_i \not\sim p_j$ per $i \neq j$. Pertanto $M_j = (p_j)$ è un ideale massimale per $j = 1, 2, \dots, n$ e $M_i \neq M_j$ per $i \neq j$. Quindi

$$I = M_1^{k_1} M_2^{k_2} \dots M_n^{k_n} = M_1^{k_1} \cap M_2^{k_2} \cap \dots \cap M_n^{k_n}.$$

Dunque

$$A/I \cong \prod_{j=1}^{n} A/M^{k_j}$$

per l'esercizio 10.21 e A/M^{k_j} è un anello locale per l'esercizio 9.30.

11.45 Per il teorema di Frobenius-Stickelberger il gruppo G è isomorfo ad un prodotto di gruppi ciclici $\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \dots \times \mathbb{Z}_{k_n}$. Scrivendo i gruppi moltiplicativamente, siano $b_1, b_2, \dots, b_n$ i generatori di questi gruppi. Allora un elemento generico di G è un monomio del tipo $b_1^{m_1} b_2^{m_2} \dots b_n^{m_n}$. Pertanto un elemento di $\mathbb{R}[G]$ avrà la forma

$$\sum_{\nu} r_\nu b_1^{m_1} b_2^{m_2} \dots b_n^{m_n},$$

dove ν denota brevemente la n-upla $(m_1, m_2, \dots, m_n)$. Possiamo definire un omomorfismo

$$\varphi : R[x_1, x_2, \dots, x_n] \to R[G]$$

ponendo

$$\varphi(f(x_1, x_2, \dots, x_n)) = \sum_{\nu} r_\nu b_1^{m_1} b_2^{m_2} \dots b_n^{m_n},$$

dove

$$f(x_1, x_2, \dots, x_n) = \sum_{\nu} r_\nu x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}.$$

Dimostrare che

$$\ker \varphi = (x_1^{k_1} - 1, x_2^{k_2} - 1, \dots, x_n^{k_n} - 1)$$

e applicare il primo teorema dell'omomorfismo.

11.46 Basta provare che $U(\mathbb{Z}_p, \cdot) \cong \mathrm{Aut}(\mathbb{Z}_p)$ è ciclico. Essendo p primo abbiamo $U(\mathbb{Z}_p) = \mathbb{Z}_p^*$, in quanto $\mathbb{F}_p = (\mathbb{Z}_p, +, \cdot)$ è un campo. Supponiamo per assurdo che $G = (\mathbb{Z}_p^*, \cdot)$ non sia ciclico. Poiché $|G| = p - 1$, al gruppo non ciclico G possiamo applicare l'esercizio 7.30. Sia d un divisore proprio di $p - 1$ tale che $x^d = 1$ per ogni $x \in G$. Allora il polinomio $f(x) = x^d - 1$ di grado d ha $p - 1 > d$ radici nel campo finito $\mathbb{F}_p$, assurdo.

11.47 Essendo $\mathrm{Aut}(\mathbb{Z}_{p^k}) \cong U(\mathbb{Z}_{p^k}, \cdot)$ dimostriamo per induzione che per ogni intero $k > 0$ il gruppo $U(\mathbb{Z}_{p^k}, \cdot)$ è ciclico, cioè esiste un intero a_k con $o_{p^k}(a_k) = p^k - p^{k-1}$, che indica brevemente il fatto che $a_k^{\varphi(p^k)} \equiv_{p^k} 1$ e $a^j \not\equiv 1_{p^k}$ per $1 < j < \varphi(p^k)$. Dall'esercizio 11.46 sappiamo che per $k = 1$ tale intero a_1 esiste. Supponiamo che

esista a_k con $o_{p^k}(a_k) = p^k - p^{k-1}$. Dimostriamo che $a_{k+1} = a_k + pt$ ha la proprietà richiesta modulo p^{k+1} per un'opportuna scelta di $t \in \mathbb{Z}$, ovvero $o_{p^{k+1}}(a_{k+1}) = p^{k+1} - p^k$. Per la scelta di a_k esiste $b \in \mathbb{Z}$ con

$$a_k^{p^k - p^{k-1}} = 1 + bp^k.$$

Vogliamo prima assicurarci che

$$o_{p^{k+1}}(a_{k+1}) \not\leq p^k - p^{k-1}. \tag{8}$$

A questo scopo calcoliamo

$$a_{k+1}^{p^k - p^{k-1}} \equiv_{p^{k+1}} a_k^{p^k - p^{k-1}} + pt(p^k - p^{k-1})a_k^{p^k - p^{k-1} - 1} \equiv_{p^{k+1}}$$

$$\equiv_{p^{k+1}} 1 + bp^k - p^k t a_k^{p^k - p^{k-1} - 1} = 1 + p^k(b - t a_k^{-1}),$$

tenuto conto della congruenza $a_k^{p^k - p^{k-1}} \equiv_{p^k} 1$. Quindi, se si sceglie $b - t a_k^{-1} \not\equiv_p 0$, ovvero $t \not\equiv_p a_k b$, si avrà (8). Sappiamo che $o_{p^{k+1}}(a_{k+1})$ non divide $p^k - p^{k-1}$, ma $o_{p^{k+1}}(a_{k+1})$ divide $p^{k+1} - p^k = p^k(p-1)$. Dunque $o_{p^{k+1}}(a_{k+1}) = p^k \cdot d$, dove d divide $p - 1$. Possiamo calcolare ora

$$a_{k+1}^{p^k \cdot d} = (a_k + pt)^{p^k \cdot d} \equiv_{p^{k+1}} a_k^{p^k \cdot d} = [a_k^{p^{k-1}}(1 + bp^k)]^d \equiv_{p^k} a_k^{p^{k-1} \cdot d}.$$

L'ipotesi

$$a_{k+1}^{p^k \cdot d} \equiv_{p^{k+1}} 1 \quad \text{implica} \quad a_k^{p^{k-1} \cdot d} \equiv_{p^k} 1,$$

che per la scelta di a_k implica $d = p - 1$. Questo dimostra $o_{p^{k+1}}(a_{k+1}) = p^{k+1} - p^k$.

13.12 Esercizi del capitolo 12

12.1 Supponiamo per assurdo che i campi $K = \mathbb{Q}(\sqrt{p})$ ed $E = \mathbb{Q}(\sqrt{q})$ siano isomorfi. Se $\varphi : K \to E$ è un tale isomorfismo, allora φ è identico su $\mathbb{Q}$. Pertanto $\sqrt{p}$, essendo una radice del polinomio $f(x) = x^2 - p$ in K, deve avere immagine $\alpha = \varphi(\sqrt{p})$ che risulta radice dello stesso polinomio in E. Verificare che E non contiene radici di $f(x)$.

12.2 Sia $\xi = \frac{-1+i\sqrt{3}}{2}$ una delle radici primitive terze dell'unità. Allora $\sqrt[3]{2}, \xi\sqrt[3]{2}$ e $\xi^2\sqrt[3]{2}$ sono le radici del polinomio $f(x) = x^3 - 2$. Pertanto il campo di spezzamento K di $f(x)$ contiene sia ξ sia $\sqrt[3]{2}$ e ovviamente coincide con $\mathbb{Q}[\xi, \sqrt[3]{2}]$.

12.3. Sia F un campo finito e siano $a_1, a_2, \ldots, a_n$ tutti gli elementi di F. Allora il polinomio

$$f(x) = (x - a_1)(x - a_2)\ldots(x - a_n) + 1 \in F[x]$$

non ha radici in F. Pertanto F non può essere algebricamente chiuso.

12.4 Si ha $x^4+4=(x^2+2x+2)(x^2-2x+2)$. Non è difficile vedere che entrambi i polinomi sono irriducibili su $\mathbb{R}$.

12.5 Poiché $u^2=5-\sqrt{5}$, $u^4-10u^2+20=0$, il polinomio $f(x)=x^4-10x^2+20$ ammette u come radice; inoltre è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein, con $p=5$. Quindi f è il polinomio minimo di u su $\mathbb{Q}$, e $[\mathbb{Q}(u):\mathbb{Q}]=4$ è il grado del polinomio minimo. Allora $1, u, u^2, u^3$ è una base per $\mathbb{Q}(u)$ su $\mathbb{Q}$: ogni elemento di $\mathbb{Q}(u)$ si scrive in modo unico come combinazione lineare $a+bu+cu^2+du^3$ con $a,b,c,d\in\mathbb{Q}$. Abbiamo un isomorfismo $\mathbb{Q}(u)\cong\mathbb{Q}[x]/(f)$ dato dalla funzione $g(u)\leftrightarrow g+(f)$. Allora è sufficiente determinare l'inverso di $x^2+(f)$ in $\mathbb{Q}[x]/(f)$. Essendo $x^2(x^2-10)\equiv-20 \operatorname{mod}(f)$, l'inverso di $x^2+(f)$ è $(10-x^2)/20+(f)$ e quindi $\frac{1}{u^2}=(10-u^2)/20$.

Per quanto riguarda la riducibilità completa, le radici di f sono $\pm\sqrt{5\pm\sqrt{5}}$. $\mathbb{Q}(u)$ è campo di spezzamento di f, poiché contiene tutti le radici di f: infatti

$$\pm\sqrt{5-\sqrt{5}}=\pm u\in\mathbb{Q}(u);$$

anche

$$\pm\sqrt{5+\sqrt{5}}\in\mathbb{Q}(u),$$

poiché

$$\sqrt{5+\sqrt{5}}=\sqrt{20}\frac{1}{u} \quad \text{e} \quad \sqrt{20}=2\sqrt{5}, \sqrt{5}=5-u^2\in\mathbb{Q}(u),$$

quindi $\sqrt{20}\in\mathbb{Q}(u)$; inoltre $\frac{1}{u}\in\mathbb{Q}(u)$, perché $u\in\mathbb{Q}(u)$ e $\mathbb{Q}(u)$ è campo.

12.6. Sia $v=u+1$, allora $\mathbb{Q}(u)=\mathbb{Q}(v)=E$. Ora $v^3=-2i\in E$ e $v^2=-\sqrt[3]{4}\in E$. Quindi i e $\sqrt[3]{2}\in E$. Poiché i ha grado 2 su $\mathbb{Q}$, mentre $\sqrt[3]{2}$ ha grado 3 su $\mathbb{Q}$, deduciamo che 6 divide $[E:\mathbb{Q}]$. D'altra parte $v^6=-4\in\mathbb{Q}$, pertanto $[E:\mathbb{Q}]\leq 6$. Questo dimostra $[E:\mathbb{Q}]=6$. Poiché $F=\mathbb{Q}(i,\sqrt[3]{2})$ contiene i e $\sqrt[3]{2}$, deduciamo come prima che 6 divide $[F:\mathbb{Q}]$. Poiché $F\leq E$, abbiamo anche $[F:\mathbb{Q}]\leq[E:\mathbb{Q}]=6$. Quindi

$$[F:\mathbb{Q}]=6 \quad \text{e} \quad E=F.$$

Da $(u+1)^6=-4$, deduciamo che u è radice del polinomio

$$f(x)=x^6+6x^5+15x^4+20x^3+15x^2+6x+5.$$

Essendo il grado di u su $\mathbb{Q}$ uguale al grado di $f(x)$, concludiamo che $f(x)$ è il polinomio minimo di u su $\mathbb{Q}$. Il polinomio minimo di u su $\mathbb{Q}(i)$ è

$$u^3+3u^2+3u+1+2i,$$

e il polinomio minimo di u su $\mathbb{Q}(\sqrt[3]{2})$ è

$$u^2+2u+1+\sqrt[3]{4}.$$

12.7 Osserviamo che $u = \sqrt[3]{2} + (\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$. Essendo

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

e $[\mathbb{Q}(u) : \mathbb{Q}] \neq 1$, risulta $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Poiché $u^3 = 6u + 6$, il polinomio $f(x) = x^3 - 6x - 6$ è il polinomio minimo di u su $\mathbb{Q}$.

12.8 Il polinomio minimo di u su $\mathbb{Q}$ è $f(x) = x^4 - 4x - 2$. Le radici di f sono

$$\pm\sqrt{2+\sqrt{6}} = \pm u \in \mathbb{Q}(u), \quad \text{e} \quad \pm i\sqrt{\sqrt{6}-2} \notin \mathbb{Q}(u).$$

Determiniamo allora il campo di spezzamento di f su $\mathbb{Q}$, estendendo $\mathbb{Q}(u)$ con la radice $\alpha = i\sqrt{\sqrt{6}-2}$. Il grado di α su $\mathbb{Q}(u)$ è 2, infatti

$$u^2 = 2 + \sqrt{6} \in \mathbb{Q}(u) \implies \sqrt{6} \in \mathbb{Q}(u) \implies 2 - \sqrt{6} \in \mathbb{Q}(u).$$

Quindi il campo di spezzamento è $K = \mathbb{Q}(i\sqrt{\sqrt{6}-2}, u)$ e

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

12.9 È facile vedere che u è radice del polinomio $f(x) = x^4 - 32x^2 + 36$ che non ha radici intere, e quindi non ha radici razionali. Supponiamo che $f(x)$ sia prodotto di due polinomi di secondo grado, cioè $f(x) = (x^2 + ax + b)(x^2 - ax + c)$ con $a, b, c \in \mathbb{Z}$. Allora si ha

$$bc = 36, \ (c-b)a = 0 \ \text{e} \ b + c - a^2 = -32. \tag{10}$$

Ora se $a = 0$, allora b, c sono soluzioni dell'equazione $x^2 + 32x + 36 = 0$, ma questa equazione non ha soluzioni intere. Quindi il caso $a = 0$ non può accadere. Se $a \neq 0$, da (10) ricaviamo $b = c = \pm 6$, da cui $b + c = \pm 12$. Di conseguenza

$$b + c - a^2 = -32$$

non può avere soluzione intera a. Questo dimostra che $f(x)$ è irriducibile. Quindi $f(x)$ è il polinomio minimo di u. Per provare che

$$\mathbb{Q}(u) = \mathbb{Q}(\sqrt{5}, \sqrt{11}),$$

basta notare che $\sqrt{5} \in \mathbb{Q}(u)$, in quanto $(u - \sqrt{5})^2 = 11$ e pertanto

$$2\sqrt{5} = u^{-1}(u^2 - 6) \in \mathbb{Q}(u).$$

Questo implica anche $\sqrt{11} \in \mathbb{Q}(u)$ e pertanto

$$E = \mathbb{Q}(\sqrt{5}, \sqrt{11}) \leq Q(u).$$

Ora

$$\sqrt{11} \notin \mathbb{Q}(\sqrt{5}) \quad \text{e} \quad \sqrt{5} \notin \mathbb{Q}(\sqrt{11}),$$

quindi E contiene propriamente $\mathbb{Q}(\sqrt{5})$ e pertanto ha grado 4. Questo dimostra $E = \mathbb{Q}(u)$. Infine, essendo

$$f(x) = (x^2 - u^2)(x^2 - \frac{36}{u^2}),$$

E contiene tutte le radici di $f(x)$.

12.10 Si consideri l'automorfismo $\lambda : \mathbb{Q}[x] \to \mathbb{Q}[x]$ dell'anello dei polinomi $\mathbb{Q}[x]$, ottenuto dalla trasformazione $x \mapsto x - 1$, cioè definito da $\lambda(g(x)) = g(x-1)$ per ogni polinomio $g(x)$. Essendo un automorfismo, λ non altera l'eventuale riducibilità. Trasformando il polinomio $f(x) = x^5 - 5x + 1$ con λ troviamo il polinomio

$$\lambda(f(x)) = x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1 - 5(x-1) + 1 =$$
$$= x^5 - 5x^4 + 10x^3 - 10x^2 + 5,$$

irriducibile per il criterio di Eisenstein. Allora anche $f(x)$ risulterà irriducibile.

12.11 Si prendano polinomi di cui già si sa che sono irriducibili, si vedano ad esempio anche i polinomi di Artin e si trasformino questi con degli automorfismi di $\mathbb{Q}[x]$ come quello descritto nell'esercizio 12.10 o ad esempio $x \mapsto x - 1/3$.

12.12 Si vede che u è radice del polinomio $f(x) = x^4 - 6x^2 - 9$ che non ha radici intere, e quindi non ha radici razionali. Supponiamo che $f(x)$ sia il prodotto di due polinomi di secondo grado, cioè $f(x) = (x^2 + ax + b)(x^2 - ax + c)$ con $a, b, c \in \mathbb{Z}$. Allora si ha

$$bc = -9, \ \ (c-b)a = 0 \ \text{ e } \ b + c - a^2 = -6.$$

Ora se $a = 0$, b, c sono soluzioni dell'equazione $x^2 + 6x - 9 = 0$, ma questa equazione non ha soluzioni intere. Quindi $a \neq 0$. Questo implica $b = c$ e $b^2 = -9$, assurdo. Pertanto $f(x)$ è irriducibile. Quindi $f(x)$ è il polinomio minimo di u. Poiché le due radici complesse di $f(x)$ non appartengono a $\mathbb{Q}(u) \subseteq \mathbb{R}$, $\mathbb{Q}(u)$ non è campo di spezzamento per $f(x)$ su $\mathbb{Q}$.

12.13 Il polinomio minimo di u su $\mathbb{Q}$ è $f(x) = x^4 + 8x^2 - 2$, irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein, con $p = 2$. Allora $[\mathbb{Q}(u) : \mathbb{Q}] = 4$. Osserviamo che

$$u = \frac{\sqrt[4]{2}}{1 + (\sqrt[4]{2})^2} \in \mathbb{Q}(\sqrt[4]{2}).$$

Il grado dell'estensione $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$ è il grado del polinomio minimo di $\sqrt[4]{2}$ su $\mathbb{Q}$, ed è 4 perché $\sqrt[4]{2}$ è radice di $x^4 - 2$, che è irriducibile per il criterio di Eisenstein e quindi $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(u)$. Infine $\mathbb{Q}(u)$ è campo di spezzamento per f se e solo se contiene tutte le radici di f. Se α è zero di f, allora

$$\alpha^4 + 8\alpha^2 - 2 = 0,$$

pertanto le radici di f sono $\pm u$ e

$$\pm i\sqrt{3\sqrt{2} + 4} \notin \mathbb{Q}(u),$$

poiché $\mathbb{Q}(u) \subseteq \mathbb{R}$. Pertanto $\mathbb{Q}(u)$ non è campo di spezzamento per f.

12.14 Questo è un polinomio di Artin.

12.15 Dimostrare che questi polinomi sono polinomi di Artin su $\mathbb{Z}$: per il polinomio $f(x)$ proiettare su $\mathbb{F}_5[x]$, per $g(x)$ su $F_7[x]$ e per $h(x)$ su $\mathbb{F}_{11}[x]$.

12.16 Essendo $\text{cont}(f) = 2$, $f(x) = 2f_1(x)$ non è primitivo, e quindi non risulta irriducibile in $\mathbb{Z}[x]$. D'altra parte, proiettando in $\mathbb{Z}_5[x]$ si trova $\overline{f}(x) = x^5 - x + 2$ quindi $f(x)$ è polinomio di Artin su $\mathbb{Z}$. Pertanto, sia $\overline{f}(x) = 2\overline{f}_1(x)$ che $\overline{f}_1(x)$ risultano irriducibili in $\mathbb{Z}_5[x]$. Questo dimostra che $f_1(x)$ è irriducibile in $\mathbb{Z}[x]$, e di conseguenza anche in $\mathbb{Q}[x]$. Essendo $f(x)$ e $f_1(x)$ associati in $\mathbb{Q}[x]$, anche $f(x)$ risulta irriducibile in $\mathbb{Q}[x]$.

12.17 Si ha $K = \mathbb{Z}_3[\alpha]$ con $\alpha^2 = -1$ e $F = \mathbb{Z}_3[\beta]$ con $\beta^2 = 1 - \beta$. Ora definiamo l'isomorfismo $\varphi : K \to F$ con $\varphi(\alpha) = 1 - \beta$. Osserviamo che $\varphi(\alpha^2) = \varphi(\alpha)^2 = -1$. Questo determina univocamente φ, poiché ogni elemento di K ha la forma $a+b\alpha$ e quindi, essendo φ identico su $\mathbb{Z}_3$, si ha

$$\varphi(a + b\alpha) = a + b\varphi(\alpha) = a + b(1 - \beta) \in F.$$

Un altro isomorfismo $\psi : K \to F$ si può definire con $\psi(\alpha) = -1 + \beta$.

12.18 Per $a = 0, 3, 4$ il polinomio ha radici. Essendo di secondo grado, questo è equivalente all'essere riducibile. Per $a = 4$ il polinomio ha radici multiple.

12.19 Questo è un polinomio di Artin su $\mathbb{Z}$ relativo al numero primo 11.

12.20 $f(x)$ non ha radici intere, e quindi non ha radici razionali. Supponiamo che $f(x)$ sia il prodotto di due polinomi di secondo grado, cioè

$$f(x) = (x^2 + ax + b)(x^2 - ax + c)$$

con $a, b, c \in \mathbb{Z}$. Allora si ha

$$bc = 1, \ (c - b)a = 0 \ \text{ e } \ b + c - a^2 = 0.$$

Ora $b = c = \pm 1$ e quindi $a^2 = \pm 2$. Questa equazione non ha soluzioni intere. Quindi $f(x)$ è irriducibile. Si noti anche che $f(x) = \Phi_8(x)$ è l'ottavo polinomio ciclotomico su $\mathbb{Q}$. Allora $(f(x))$ è un ideale massimale, quindi K è un campo e $[K : \mathbb{Q}] = \deg f(x) = 4$. Ora $K = \mathbb{Q}(\alpha)$, dove $\alpha^4 = -1$, quindi α^2 è radice del polinomio x^2+1. Pertanto x^2+1 non è irriducibile su K. D'altra parte, $z = \alpha(1-\alpha^2)$ è radice del polinomio $x^2 - 2$, quindi neanche $x^2 - 2$ è irriducibile.

12.21 La proiezione in $\mathbb{Z}_2[x]$ del polinomio $f(x)$ è $\overline{f}(x) = x^7 + x^5 + x^3 + x +$ [illegible]
Questo polinomio non ha radici in $\mathbb{Z}_2$. Inoltre non è divisibile per gli unici polin[illegible] irriducibili

$$x^2 + x + 1, \quad x^3 + x^2 + 1 \quad \text{e} \quad x^3 + x + 1 \quad \text{di grado } \leq 3.$$

Infatti

$$\overline{f}(x) = x^3(x^2+x+1)^2 + x + 1 =$$
$$= x(x^3+x^2+1)^2 + x^3 + 1 = x^5(x^2+1) + x^3 + x + 1.$$

Quindi $\overline{f}(x)$ è irriducibile su $\mathbb{Z}_2$. Questo dimostra che $f(x)$ è irriducibile su $\mathbb{Z}$.

Il grado di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$ è 7, pertanto ogni sottocampo di $\mathbb{Q}(\alpha)$, che contiene propriamente $\mathbb{Q}$, deve coincidere con $\mathbb{Q}(\alpha)$, essendo 7 un numero primo e quindi privo di divisori propri. Essendo α^3 un elemento di $\mathbb{Q}(\alpha)$ che non appartiene a $\mathbb{Q}$, si ha $\mathbb{Q}(\alpha^3) = \mathbb{Q}(\alpha)$.

12.25 Le radici n-esime dell'unità formano un sottogruppo finito e quindi ciclico del gruppo moltiplicativo del campo. Le radici primitive sono i generatori di tale gruppo che è isomorfo al gruppo additivo di $\mathbb{Z}/n\mathbb{Z}$.

12.27 Poiché $g_{a,b}$ non deve avere radici, risulta $g_{a,b}(1) = a + b + 1 \neq 0$. Quindi $a+b = 0$ e, di conseguenza, $b = a$. Per provare che il polinomio $g_{a,a}$ sia irriducibile, basta assicurarsi che $g_{a,a}$ non sia divisibile per gli unici polinomi irriducibili su $\mathbb{Z}_2$ di grado maggiore di 1 e minore o uguale a 3:

$$q(x) = x^2 + x + 1, \quad h_1(x) = x^3 + x + 1 \quad \text{e} \quad h_2(x) = x^3 + x^2 + 1.$$

Poiché

$$g_{a,a}(x) = x^7 + x^3 + ax^2 + ax + 1$$

è congruo a $ax^2 + ax + x$ modulo $q(x)$, è chiaro che $q(x)$ non divide mai $g_{a,a}$. Analogamente $g_{a,a}(x)$ è congruo ad $ax^2 + (a+1)x + 1$ modulo $h_1(x)$ e è congruo a $(a+1)x^2 + ax + 1$, modulo $h_2(x)$. Quindi né $h_1(x)$ né $h_2(x)$ dividono $g_{a,a}$. Pertanto $g_{a,a}$ è irriducibile per $a = 0$ e $a = 1$.

12.28 Osserviamo che α è radice del polinomio

$$g(x) = x^3 - 3\sqrt{2}x^2 + 6x - 2\sqrt{2} - 5 \in E[x], \text{ con } E = \mathbb{Q}(\sqrt{2}).$$

Poiché $\alpha \notin E$ (verificare), il grado di α su E deve essere 3, quindi $g(x)$ è il polinomio minimo di α su E. Si ragioni analogamente per il polinomio minimo $f \in \mathbb{Q}[x]$.

12.29 Nella formula del lemma 12.49 isolare il prodotto $f(x)$ di tutti termini $\Phi_d(x)$ con $d|n$, $d \neq n$ e $d \not| k$. Applicando la stessa formula a k si ottiene

$$x^k - 1 = \prod_{d|k} \Phi_d(x),$$

quindi

$$x^n - 1 = \Phi_n(x) \cdot f(x) \cdot (x^k - 1).$$

Allora

$$\frac{x^n - 1}{x^k - 1} = \Phi_n(x) \cdot f(x)$$

è divisibile per $\Phi_n(x)$.

12.30 Il gruppo moltiplicativo F^* ha $n-1$ elementi, pertanto $a^{n-1} = 1$ per ogni elemento $a \in F^*$. In altre parole ogni elemento non nullo di F è radice del polinomio $x^{n-1} - 1$. D'altra parte ogni elemento non nullo di F è radice anche del polinomio

$$f(x) = (x - a_1)(x - a_2) \dots (x - a_{n-1}).$$

Poiché questi polinomi sono monici e di grado $n - 1$, il fatto che abbiano le stesse $n-1$ radici distinte $a_1, \dots, a_{n-1}$ permette di concludere che coincidono. Quindi -1 coincide con il termine noto $a_1 \dots a_{n-1}$ di $f(x)$.

12.31 Da $|F| = 9$ segue char $F = 3$. Il gruppo moltiplicativo F^* ha 8 elementi, pertanto $a^8 = 1$ per ogni elemento $a \in F^*$, da cui

$$0 = a^8 - 1 = (a^2)^4 - 1^4 = (a^2 - 1)(a^6 + a^4 + a^2 + 1). \tag{11}$$

Se $a \neq \pm 1$, si ha $a^2 - 1 \neq 0$ e quindi (11) permette di concludere $a^6 + a^4 + a^2 + 1 = 0$.

12.32 Dimostrare che il polinomio $x^4 + 2$ è irriducibile su $\mathbb{F}_5$.

12.33 Sia $K = \mathbb{Z}_{11}[x]/(x^2 + 1)$ e $F = \mathbb{Z}_{11}[x]/(x^2 + x + 4)$. Allora $K = \mathbb{Z}_{11}[\alpha]$ ed $E = \mathbb{Z}_{11}[\beta]$ con $\alpha^2 = -1$ e $\beta^2 + \beta + 4 = 0$. Allora definiamo l'isomorfismo $\varphi : K \to F$ con $\varphi(\alpha) = \pm(5 - \beta)$. Basta verificare che $\varphi(\alpha^2) = \varphi(\alpha)^2 = -1$.

12.35 Applicando il teorema 12.61 si ricava $x^9 - x$.

12.36 I numeri 6, 10, 12, 14, 15, 18 e 20 non possono essere cardinalità di un campo finito, perché non sono potenze di numero primo. Per i numeri primi 5, 7, 11, 13, 17 e 19 basta prendere il rispettivo $\mathbb{F}_p$. Per 4 e 9 si applichi l'esempio 12.10, per 8 e 16 si considerino i quozienti $\mathbb{Z}_2[x]/(x^3 + x + 1)$ e $\mathbb{Z}_2[x]/(x^4 + x^3 + 1)$ rispettivamente.

12.37 Il polinomio $f(x) = x^4 - 5$ è irriducibile per il criterio di Eisenstein. Dall'uguaglianza

$$(x^2 + 1)(x^2 - 1) = x^4 - 1 \in 4 + (f(x))$$

ricaviamo

$$(x^2 + 1 + (f(x)))^{-1} = \frac{x^2 - 1}{4} + (f(x)).$$

12.38 Si applichi il teorema 12.61 con $m = p$ e $g(x) = f_a(x)$, sfruttando il fatto che $f_a(x)$ è irriducibile (vedi teorema 12.56).

12.41 Si ha $\Phi_{12}(x) = x^4 - x^2 + 1$, $\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$, $\Phi_{40}(x) = x^{16} - x^{12} + x^8 - x^4 + 1$, $\Phi_{60}(x) = x^{16} + x^{14} - x^{10} - x^8 - x^6 + x^2 + 1$.

12.43 Per dimostrare che per $n > 1$ si ha $\sum_{d|n} \mu(d) = 0$, si consideri prima il caso facile in cui $n = p^k$, dove p è primo. Nel caso generale si può ragionare per induzione sul numero dei primi che dividono n.

12.44 Applicare la formula di inversione di Möbius alla formula $n = \sum_{d|n} \varphi(d)$.

12.45 Si applichi il fatto che π è trascendente.

12.46 Il polinomio è riducibile per tutti gli interi k della forma $k = \pm 2 - a^2$, dove $a \in \mathbb{Z}$. Si scriva $f(x) = (x^2 + ax + b)(x^2 - ax + c)$ e si noti che $bc = 1$ implica $b = c = \pm 1$ e quindi $b + c = \pm 2$. Uguagliando i coefficienti di x^2 si ricava $k = \pm 2 - a^2$.

12.47 Dimostrare per induzione su k, che se $f(x) = (x - \alpha)^k f_1(x)$, allora esiste un polinomio $f_2(x) \in K[x]$, tale che

$$f^{(k)}(x) = (x - \alpha) f_2(x) + k! f_1(x). \qquad (*)$$

Ora, se α è radice di $f(x), f'(x), \ldots, f^{k-1}(x)$ dimostriamo per induzione su k che α è una radice di molteplicità $\geq k$ di $f(x)$. Per $k = 1$ l'asserto è banale. Supponiamo $k > 1$ e l'asserto vero per $k - 1$, quindi da

$$f(\alpha) = f'(\alpha) = \ldots = f^{k-2}(\alpha) = 0$$

concludiamo che α è una radice di molteplicità $\geq k - 1$ di $f(x)$. Quindi, $f(x) = (x - 1)^{k-1}(x) f_1(x)$ per qualche $f_1(x) \in K[x]$. Da $(*)$ applicato a $k - 1$ deduciamo

$$f^{(k-1)}(x) = (x - \alpha) f_2(x) + (k - 1)! f_1(x)$$

per un opportuno polinomio $f_2(x) \in K[x]$. Sostituendo con $x = \alpha$, da $f^{k-1}(\alpha) = 0$ ricaviamo $(k - 1)! f_1(\alpha) = 0$. Poiché K ha caratteristica zero, concludiamo che $f_1(\alpha) = 0$. Quindi $f_1(x) = (x - \alpha) f_3(x)$ per qualche $f_3(x) \in K[x]$. Pertanto $f(x) = (x - 1)^k(x) f_3(x)$ e quindi α è una radice di molteplicità $\geq k$ di $f(x)$.

12.48 Sia $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$ con $a_i \in K$ e $a_m \neq 0$. Se K avesse caratteristica zero, allora $m a_m \neq 0$. Quindi la nostra ipotesi $f'(x) = 0$ implica char $K = p$ per qualche primo p. L'ipotesi $f'(x) = 0$ implica anche $j a_j = 0$ per ogni $j = 0, 1, \ldots, m$. Quindi $p | j$ per tutti i j con $a_j \neq 0$. Pertanto $f(x)$ ha la forma $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \ldots + a_{kp} x^{kp}$. Quando K è finito, ogni $a \in K$ ha la forma $a = b^p$ per qualche $b \in K$ poiché l'applicazione $a \mapsto a^p$ è iniettiva e quindi anche suriettiva. Allora, scrivendo ogni a_{ip} come $a_{ip} = b_i^p$, con $b_i \in K$, si ricava $f(x) = g(x)^p$, dove $g(x) = b_0 + b_1 x^p + b_2 x^2 + \ldots + b_k x^k$.

12.49 Ogni numero reale algebrico α è radice di un polinomio $f(x)$ su $\mathbb{Q}$. Quindi α è determinato da un insieme finito di numeri razionali, i coefficienti del polinomio $f(x)$. La famiglia di tutti gli insiemi finiti di numeri razionali è numerabile. Quindi anche l'insieme degli elementi algebrici α è numerabile.

12.50 Sia ξ una radice primitiva n-esima di 1. Allora le radici di $\Phi_n(x)$ sono ξ^k, dove $1 \leq k \leq n$ è coprimo con n. Poiché $\varphi(\xi)$ resta una radice primitiva n-esima di 1 per ogni automorfismo φ di K, si ha $\varphi(\xi) = \xi^k$ per un certo $1 \leq k \leq n$ coprimo con n. Inoltre il valore $\varphi(\xi)$ determina completamente ξ. Quindi $\mathrm{Aut}(K)$ è isomorfo al gruppo degli automorfismi del gruppo ciclico $\mathbb{Z}_n$, studiato nel paragrafo 7.1.

12.51 Per l'esercizio 11.44

$$\mathbb{R}[G] \cong \mathbb{R}[x]/(x^n - 1).$$

Se $n = 2k + 1$, il polinomio $f(x) = x^n - 1$ si fattorizza in

$$f(x) = (x-1)f_1(x)f_2(x)\dots f_k(x),$$

dove $f_j(x)$ sono fattori irriducibili di grado 2. Pertanto, l'ideale principale $I = (f(x))$ di $\mathbb{R}[x]$ soddisfa

$$I = M_0 M_1 M_2 \dots M_k = M_0 \cap M_1 \cap M_2 \cap \dots \cap M_k,$$

dove $M_0 = (x-1)$ e $M_j = (f_j(x))$ per $j = 1, 2, \dots, k$. Quindi

$$\mathbb{R}[x]/I \cong \mathbb{R}/M_0 \times \mathbb{R}/M_1 \times \dots \times \mathbb{R}/M_k.$$

Essendo

$$R/M_0 \cong \mathbb{R} \text{ e } \mathbb{R}/M_j \cong \mathbb{C}$$

per $j = 1, 2, \dots, k$ concludiamo che $\mathbb{R} \times \mathbb{C}^k$. L'altro caso è analogo.

12.52 Per l'esercizio 11.44 si ha $\mathbb{Q}[G] \cong \mathbb{Q}[x]/(x^n - 1)$. Sappiamo che

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

è la fattorizzazione di $x^n - 1$ in fattori irriducibili in $\mathbb{Q}[x]$. Pertanto l'ideale principale $I = (x^n - 1)$ di $\mathbb{Q}[x]$ soddisfa

$$I = \prod_{d|n} M_d = \bigcap_{d|n} M_d,$$

dove $M_d = (\Phi_d(x))$ per $d|n$ e M_d è massimale. Quindi

$$\mathbb{Q}[x]/I \cong \prod_{d|n} \mathbb{Q}[x]/M_d.$$

Essendo $\mathbb{Q}[x]/M_d \cong \mathbb{Q}(\xi_d)$ per $d|n$ concludiamo che

$$\mathbb{Q}[G] \cong \prod_{d|n} \mathbb{Q}(\xi_d).$$

12.53 Per l'esercizio 11.44 si ha $\mathbb{Q}[G] \cong \mathbb{Q}[x]/(x^8 - 1)$. Sappiamo che

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$$

è la fattorizzazione di $x^8 - 1$ in fattori irriducibili in $\mathbb{Q}[x]$. Allora gli ideali

$$M_1 = (x-1), \; M_2 = (x+1), \; M_3 = (x^2+1) \; \text{ e } \; M_4 = (x^4+1)$$

sono massimali e l'ideale principale $I = (x^8 - 1)$ di $\mathbb{Q}[x]$ soddisfa

$$I = M_1 \cap M_2 \cap M_3 \cap M_4.$$

Quindi

$$\mathbb{Q}[x]/I \cong \prod_{j=1}^{4} \mathbb{Q}[x]/M_j.$$

Essendo $\mathbb{Q}[x]/M_i \cong \mathbb{Q}$ per $j = 1, 2$ concludiamo che

$$\mathbb{Q}[G] \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}[i] \times \mathbb{Q}[\eta],$$

dove i è identità immaginaria e η è una radice primitiva quarta dell'unità.

12.54 (a) Faremo uso dell'isomorfismo $K[G] \cong K[x]/I$, dove $I = (x^n - 1)$. Supponiamo che $x^n - 1 = \prod_{j=1}^{s} f_j(x)$ sia la decomposizione in prodotto di irriducibili in $K[x]$. Poiché il polinomio $x^n - 1$ non ha radici multiple, in quanto la sua derivata non ha zeri in comune con $x^n - 1$, si ha che i polinomi f_j sono tutti distinti. Allora

$$I = M_1 M_2 \dots M_s,$$

dove $M = (f_j(x))$ è l'ideale massimale generato dal polinomio irriducibile $f_j(x)$ di grado d_j su K. Osserviamo che $\sum_{i=1}^{s} d_i = n$. Per l'esercizio 10.18 (b) si ha $K[x]/I \cong \prod_j F_j$, dove F_j è il campo $K[x]/M_j$ di grado d_j. Osserviamo che se $\eta_1 = 1, \eta_2, \dots, \eta_t$ sono tutte le radici n-esime di 1 contenute nel campo K, allora i rispettivi polinomi $f_1(x), \dots, f_t(x)$ sono della forma $f_j(x) = x - \eta_j$, e quindi $F_j \cong K$ per ogni $j = 1, \dots, t$.

(b) Se il campo è algebricamente chiuso, $F_j \cong K$ e $d_j = 1$ per ogni $j = 1, \dots, s$, da cui $K[G] \cong K^n$.

12.55 Sia $A = K[x_1, x_2, \dots, x_n]$. Per l'esercizio 11.45 l'anello $K[G]$ è isomorfo a A/I, dove

$$I = (x_1^2 - 1, x_2^2 - 1, \dots, x_n^2 - 1).$$

Sia $\varepsilon = (e_1, e_2, \dots, e_n)$ una n-upla di ± 1: notiamo che ci sono 2^n di tali n-uple. Poniamo

$$M_\varepsilon = (x_1 + e_1, x_2 + e_2, \dots, x_n + e_n)$$

per ogni ε. Allora

$$I = \bigcap_\varepsilon M_\varepsilon.$$

Pertanto

$$A/I \cong \prod_\varepsilon A/M_\varepsilon \cong K^{2^n}$$

essendo $A/M_\varepsilon \cong K$ per ogni ε.

Per un'altra soluzione per induzione su n si potrebbero utilizzare gli esercizi 10.25 e 10.29.

12.56 Sia $A = \mathbb{R}[x, y]$. Per l'esercizio 11.45 l'anello $\mathbb{R}[G]$ è isomorfo a A/I, dove

$$I = (x^3 - 1, y^3 - 1).$$

Siano

$$N_0 = (x-1, y-1), \quad N_1 = (x-1, y^2+y+1), \quad N_2 = (y-1, x^2+x+1),$$

$$M_1 = (x^2+x+1, x-y) \text{ ed } M_2 = (x^2+x+1, x-y).$$

Per lo svolgimento dell'esercizio 11.41 l'ideale

$$J = (x^2+x+1, y^2+y+1) \text{ coincide con } M_1 \cap M_2 = M_1 M_2.$$

Essendo $I = N_0 N_1 N_2 J$, ricaviamo

$$I = N_0 N_1 N_2 M_1 M_2 = N_0 \cap N_1 \cap N_2 \cap M_1 \cap M_2.$$

Per l'esercizio 10.21

$$A/I \cong A/N_0 \times A/N_1 \times A/N_2 \times A/M_1 \times A/M_2.$$

Poiché

$$A/N_0 \cong \mathbb{R} \text{ e } A/N_i \cong A/M_i \cong \mathbb{C}$$

per $i = 1, 2$, troviamo

$$\mathbb{R}[G] \cong \mathbb{R} \times \mathbb{C}^4.$$

Glossario

$\binom{n}{k}$	coefficiente binomiale, 22
$\aleph_0$	cardinale numerabile, 35
$\lfloor \rho \rfloor$	parte intera di ρ, 50
(a, b)	massimo comun divisore di a e b, 61
$[G : H]$	indice di H in G, 125
$\trianglelefteq$	sottogruppo normale, 128
$\downarrow a$	ideale generato da a in un reticolo, 242
2^X	funzioni di X in $\{0, 1\}$, 8
A^I	potenza cartesiana, 31
A_n	gruppo alterno su n elementi, 119
A^t	matrice trasposta di A, 134
$\mathrm{Aut}(G)$	gruppo degli automorfsimi del gruppo G, 153
A^*	insieme degli elementi non nulli di un anello A, 212
$A[b]$	sottoanello generato da A e da b, 219
$\mathbb{B} = \{0, 1\}$	minimo reticolo booleano, 241
C_k^n	coefficiente binomiale, 22
$\mathbb{C}$	numeri complessi, 51
$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$	numeri complessi non nulli, 95
$C_G(X)$	centralizzante di X in G, 188
$\mathrm{cont}\,(f)$	contenuto di f, 270
$\mathrm{D}_n(K)$	gruppo delle matrici diagonali, 132
D_8	gruppo diedrale di ordine 8, 142
$\exp(G)$	esponente del gruppo G, 127
$\mathrm{End}(G)$	insieme degli endomorfismi del gruppo G, 153

$\varphi(n)$	funzione di Eulero, 76
$f_{K,\alpha}$	polinomio minimo di un elemento algebrico α su K, 287
$GL_n(K)$	gruppo generale lineare di dimensione n su K, 104
G_x	stablizzatore di x, 198
$h(L)$	altezza di un insieme parzialmente ordinato L, 43
$Hom(G,H)$	insieme degli omomorfismi di gruppo di G in H, 152
H^G	chiusura normale di H in G, 189
H_G	cuore di H in G, 187
$I_X(x)$	segmento iniziale di X, 29
$\mathrm{Inn}(G)$	gruppo degli automorfismi interni del gruppo G, 153
$\mathcal{J}(L)$	insieme degli ideali di un reticolo distributivo limitato, 243
$\mathcal{L}(G)$	reticolo dei sottogruppi del gruppo G, 122
$m.c.m.(a,b)$	minimo comune multiplo di a e b, 61
$M_{m\times n}(R)$	matrici $m \times n$ a coefficienti in R, 98
$M_n(R)$	matrici $n \times n$ a coefficienti in R, 98
$\mathbb{N}$	numeri naturali, 13
$n!$	fattoriale, 16
$\mathcal{N}(G)$	reticolo dei sottogruppi normali, 130
$N_p(n)$	numero dei polinomi irriducibili monici di grado n sul campo $\mathbb{F}_p$, 305
$o_p(a)$	ordine di a modulo p, 76
$o(x)$	ordine dell'elemento x, 109
$\mathrm{O}_n(K)$	gruppo ortogonale lineare, 134
Ω_G	insieme dei punti fissi di G in Ω, 198
$[\Omega]^n$	l'insieme dei sottoinsiemi di Ω di cardinalità n, 200
$\mathcal{P}(X)$	insieme delle parti di X, 3
$P(A)$	insieme dei rappresentanti degli elementi irriducibili di un anello A, 260

$\mathbb{Q}$	numeri razionali, 49
$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$	numeri razionali non nulli, 95
Q_8	gruppo dei quaternioni, 135
$\mathbb{R}$	numeri reali, 50
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$	numeri reali non nulli, 95
S_X	insieme delle permutazioni di un insieme X, 110
S_n	gruppo simmetrico su n oggetti, 111
$Syl_p(G)$	insieme dei p-sottogruppi di Sylow di G, 127
$SL_n(K)$	gruppo speciale lineare, 132
$\mathrm{T}_n^+(K)$	gruppo delle matrici triangolari superiori, 132
$U(M)$	insieme degli elementi invertibili del monoide M, 106
Y^X	insieme delle applicazioni da X a Y, 7
$\mathbb{Z}$	numeri interi, 47
$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$	numeri interi non nulli, 60
$Z(G)$	centro del gruppo G, 131

Indice analitico